AHKAM
Jurnal Hukum Islam dan Humaniora

p-ISSN: 2964-6332
e-ISSN: 2964-6340

Terindeks: Dimensions, Scilit, Lens, Semantic, Crossref Garuda, Google, Base, etc.

https://doi.org/10.58578/ahkam.v5i2.9511

PERLINDUNGAN HUKUM TERHADAP KEAMANAN DATA NASABAH BANK MANDIRI DARI KEJAHATAN *PHISHING*

Legal Protection of Bank Mandiri Customer Data Security Against Phishing Crimes

Fitria Wulandari, Dianne Eka Rusmawati, M. Wendy Trijaya, Maya Shafira, Dinda Anna Zatika
Universitas Lampung
wulan.fitria2002@gmail.com; dianne.eka@fh.unila.ac.id

Article Info:

Submitted:	Revised:	Accepted:	Published:
Feb 27, 2026	Mar 27, 2026	Apr 8, 2026	Apr 13, 2026

Abstract

Although the issue of personal data protection in the banking sector has received attention in various studies, studies that specifically examine the integration of the normative, ideal, and factual roles of banking in preventing phishing crimes remain limited. This study aims to analyze the role of Bank Mandiri in protecting customer data security from phishing crimes and to evaluate the effectiveness of legal protection based on laws and regulations in Indonesia. This study employed a qualitative approach with a case study design through a normative juridical method. Data were collected through library research and document analysis, and were then analyzed using descriptive-analytical techniques. The results show that Bank Mandiri has implemented comprehensive protection measures, including compliance with regulations, the use of advanced security technology, and customer education. In addition, the legal framework in Indonesia has provided preventive and repressive protection through various regulations governing data protection and cybercrime. These findings contribute to the development of legal protection theory and institutional responsibility in cybersecurity governance. This study concludes that

synergy among banking institutions, regulators, and customers plays an important role in minimizing phishing risks. Therefore, improvements in cybersecurity infrastructure and the strengthening of digital literacy programs are needed to reinforce the protection of customer data. The implications of this study include theoretical contributions in the field of law and practical recommendations for strengthening data protection policies, while also opening opportunities for further studies on cross-sector collaboration and technological innovation in the financial sector.

Keywords: Banking Security; Cybercrime; Personal Data Protection; Legal Protection; Phishing

Abstrak: Meskipun isu perlindungan data pribadi di sektor perbankan telah menjadi perhatian dalam berbagai penelitian, kajian yang secara khusus menelaah integrasi peran normatif, ideal, dan faktual perbankan dalam mencegah kejahatan *phishing* masih terbatas. Penelitian ini bertujuan untuk menganalisis peran Bank Mandiri dalam melindungi keamanan data nasabah dari kejahatan *phishing* serta mengevaluasi efektivitas perlindungan hukum berdasarkan peraturan perundang-undangan di Indonesia. Penelitian ini menggunakan pendekatan kualitatif dengan desain studi kasus melalui metode yuridis normatif. Data dikumpulkan melalui studi kepustakaan dan analisis dokumen, kemudian dianalisis menggunakan teknik deskriptif-analitis. Hasil penelitian menunjukkan bahwa Bank Mandiri telah menerapkan langkah-langkah perlindungan yang komprehensif, meliputi kepatuhan terhadap regulasi, penggunaan teknologi keamanan yang canggih, serta edukasi kepada nasabah. Selain itu, kerangka hukum di Indonesia telah memberikan perlindungan preventif dan represif melalui berbagai peraturan yang mengatur perlindungan data dan kejahatan siber. Temuan ini berkontribusi terhadap pengembangan teori perlindungan hukum dan tanggung jawab institusi dalam tata kelola keamanan siber. Penelitian ini menyimpulkan bahwa sinergi antara lembaga perbankan, regulator, dan nasabah memegang peran penting dalam meminimalkan risiko *phishing*. Oleh karena itu, peningkatan infrastruktur keamanan siber dan penguatan program literasi digital diperlukan untuk memperkuat perlindungan data nasabah. Implikasi penelitian ini mencakup kontribusi teoretis dalam bidang hukum serta rekomendasi praktis bagi penguatan kebijakan perlindungan data, sekaligus membuka peluang kajian lanjutan mengenai kolaborasi lintas sektor dan inovasi teknologi di sektor keuangan.

Kata Kunci: Keamanan Perbankan; Kejahatan Siber; Perlindungan Data Pribadi; Perlindungan Hukum; *Phishing*

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah membawa transformasi signifikan dalam berbagai aspek kehidupan, termasuk sektor perbankan yang kini semakin terdigitalisasi melalui layanan *electronic banking (e-banking)*. Inovasi ini memberikan kemudahan, kecepatan, dan efisiensi dalam melakukan transaksi keuangan, seperti transfer dana, pembayaran tagihan, hingga pengelolaan deposito secara daring. Namun, di balik kemudahan tersebut, muncul isu krusial berupa meningkatnya ancaman kejahatan siber, khususnya *phishing*, yang menargetkan data pribadi dan finansial nasabah. Phising sendiri merupakan

bentuk kejahatan siber (*cybercrime*) yang bertujuan memperoleh data sensitif melalui penipuan yang terstruktur. Istilah "*phising*" berasal dari kata "*fishing*" (memancing), yang menggambarkan metode pelaku dalam "memancing" korban agar menyerahkan informasi penting secara sukarela. Pelaku umumnya menggunakan email, pesan singkat, atau situs web palsu yang menyerupai tampilan resmi bank guna mengelabui korban. Dalam beberapa kasus, *phising* juga melibatkan penyisipan kode berbahaya yang dapat dimanfaatkan untuk mengambil alih sesi login atau informasi penting lainnya (Yudha et al., 2018).

Kejahatan *phising* termasuk ke dalam kategori penipuan sebagaimana diatur dalam Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP) mengatur bahwa penipuan adalah perbuatan dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum dengan menggunakan tipu muslihat, nama palsu, atau rangkaian kebohongan yang mengakibatkan kerugian bagi pihak lain. Dalam konteks phising, kejahatan ini dilakukan dengan memanfaatkan teknologi informasi dan komunikasi, seperti internet, media sosial, atau aplikasi digital, untuk menipu korban. *Phising* merupakan salah satu jenis kejahatan siber yang melanggar hukum sebagaimana diatur dalam Pasal 30 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik selanjutnya disingkat UU ITE yang mengatur bahwa setiap orang yang dengan sengaja, tanpa hak, atau melawan hukum mengakses komputer atau sistem elektronik milik orang lain dengan cara apa pun, baik untuk memperoleh informasi atau dokumen elektronik, maupun dengan melanggar atau merusak sistem pengamanan, dapat dianggap melakukan kejahatan. Pelanggaran terhadap pasal ini dapat mengakibatkan hukuman penjara dengan maksimal 8 (delapan) tahun dan/atau denda hingga Rp800.000.000,00 (delapan ratus juta rupiah).

Data dari Anti Phishing Working Group (APWG) menunjukkan bahwa jumlah serangan *phishing* secara global terus meningkat, bahkan mencapai lebih dari satu juta kasus dalam satu kuartal pada periode 2024- 2025. Di Indonesia sendiri, tingginya angka percobaan *phishing* menunjukkan bahwa masyarakat masih rentan terhadap serangan tersebut, sehingga isu perlindungan data nasabah dalam sistem *e-banking* menjadi sangat relevan untuk dikaji (Wibowo et al., 2023). *Phising* dalam sektor perbankan merupakan bentuk kejahatan siber yang dilakukan untuk mencuri data pribadi dan finansial nasabah dengan menyamar sebagai pihak resmi bank. Bentuknya beragam, mulai dari *email phising*, *smishing* (melalui SMS), *vishing* (melalui telepon), hingga situs web dan aplikasi palsu yang menyerupai layanan resmi

perbankan. *Email phising* umumnya memuat tautan yang mengarahkan penerima ke situs web palsu yang dirancang sedemikian rupa oleh pelaku untuk menyerupai situs resmi, dengan maksud memperoleh informasi pribadi nasabah, seperti kata sandi, nomor kartu kredit, serta data rahasia lainnya. (Idris Balaka et al., 2024).

Berdasarkan fenomena tersebut, peneliti memandang bahwa perkembangan teknologi dalam sektor perbankan merupakan pedang bermata dua yang tidak hanya memberikan manfaat, tetapi juga menimbulkan risiko yang signifikan terhadap keamanan data pribadi nasabah. Teori perlindungan hukum yang dikemukakan oleh Philipus M. Hadjon menegaskan bahwa negara memiliki kewajiban untuk memberikan perlindungan terhadap hak-hak subjek hukum melalui instrumen hukum yang ada (Hadjon, 2011). Selain itu, pandangan C.S.T. Kansil juga menekankan pentingnya peran aparat penegak hukum dalam memberikan rasa aman kepada masyarakat dari berbagai ancaman, termasuk kejahatan siber. Dengan demikian, keberadaan regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, dan Undang-Undang Perbankan harus mampu menjawab tantangan perkembangan kejahatan *phishing* yang semakin kompleks dari waktu ke waktu (Alsayed & Bilgrami, 2017).

Sejumlah penelitian sebelumnya telah mengkaji perlindungan hukum terhadap data pribadi dalam transaksi elektronik dan sektor perbankan. Namun, sebagian besar penelitian tersebut masih berfokus pada aspek normatif secara umum tanpa mengkaji secara spesifik efektivitas perlindungan hukum terhadap kasus *phishing* dalam praktik perbankan digital. Selain itu, penelitian terdahulu juga cenderung belum mengaitkan secara komprehensif antara regulasi yang ada dengan implementasi perlindungan nasabah dalam kasus konkret, khususnya yang melibatkan bank besar seperti Bank Mandiri. Hal ini menunjukkan adanya kesenjangan penelitian (*research gap*) yang perlu diisi, terutama dalam menganalisis sejauh mana perlindungan hukum yang ada mampu memberikan jaminan keamanan data bagi nasabah di tengah maraknya kejahatan siber.

Kebaruan dalam penelitian ini terletak pada pendekatan analisis yang tidak hanya menelaah aspek normatif dari peraturan perundang-undangan, tetapi juga mengkaji implementasi perlindungan hukum dalam kasus nyata *phishing* yang menimpa nasabah Bank Mandiri. Penelitian ini menggunakan teori perlindungan hukum sebagai landasan utama, dengan membedakan antara perlindungan hukum preventif dan represif dalam konteks kejahatan siber di sektor perbankan. Selain itu, penelitian ini juga mengintegrasikan konsep

perlindungan data pribadi dalam sistem digital dengan prinsip kerahasiaan bank sebagaimana diatur dalam Undang-Undang Perbankan, sehingga memberikan perspektif yang lebih komprehensif dalam melihat perlindungan nasabah. Bank memiliki kewajiban untuk menjaga kerahasiaan seluruh data dan informasi yang diperoleh dalam menjalankan kegiatan usahanya, baik yang berkaitan dengan orang maupun badan hukum (Asril, 2018). Berdasarkan uraian tersebut, penelitian ini difokuskan pada analisis perlindungan hukum terhadap keamanan data nasabah Bank Mandiri dari kejahatan *phishing*. Adapun tujuan penelitian ini adalah untuk mengkaji dan menganalisis bentuk perlindungan hukum yang diberikan kepada nasabah, mengevaluasi efektivitas regulasi yang berlaku dalam menghadapi kejahatan *phishing*, serta memberikan rekomendasi untuk memperkuat sistem perlindungan data nasabah di era digital. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi akademik maupun praktis dalam pengembangan hukum di bidang perlindungan konsumen dan keamanan data di sektor perbankan.

METODE

Metode penelitian dalam kajian ini disusun secara sistematis untuk memperoleh hasil yang valid, objektif, dan dapat dipertanggungjawabkan secara ilmiah. Metode penelitian dipahami sebagai suatu cara kerja ilmiah yang digunakan untuk mengkaji permasalahan hukum melalui tahapan yang terstruktur, mulai dari pengumpulan data hingga analisis, guna menjawab rumusan masalah penelitian secara tepat. Dalam konteks penelitian ini, metode yang digunakan mengintegrasikan pendekatan normatif dan empiris agar mampu memberikan gambaran yang komprehensif terkait perlindungan hukum terhadap keamanan data nasabah dari kejahatan *phishing* dalam sektor perbankan (Efendi et al., 2016).

Penelitian ini menggunakan jenis penelitian hukum normatif-empiris dengan karakteristik utama mengkaji hukum tidak hanya sebagai norma tertulis (*law in books*), tetapi juga sebagai praktik nyata dalam masyarakat (*law in action*). Pendekatan ini memungkinkan peneliti untuk menganalisis kesesuaian antara ketentuan peraturan perundang-undangan dengan implementasinya dalam kasus konkret, khususnya terkait perlindungan data nasabah Bank Mandiri dari kejahatan *phishing*. Dengan demikian, penelitian ini tidak hanya bersifat teoritis, tetapi juga aplikatif dalam menilai efektivitas hukum yang berlaku.

Desain penelitian yang digunakan adalah deskriptif kualitatif, yang bertujuan untuk memberikan gambaran secara sistematis, faktual, dan mendalam mengenai fenomena hukum

yang diteliti. Rancangan ini dipilih karena mampu menjelaskan secara komprehensif kondisi perlindungan hukum terhadap data nasabah dalam praktik perbankan digital. Penelitian ini juga mengombinasikan beberapa pendekatan, yaitu pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*), sehingga analisis yang dihasilkan dapat mencakup aspek normatif, teoritis, dan empiris secara terpadu (Kadarudin & MH, 2021).

Partisipan dalam penelitian ini terdiri dari dua narasumber yang memiliki kompetensi dan pengalaman relevan di bidang keamanan sistem perbankan dan desain layanan digital. Narasumber tersebut adalah pegawai PT Bank Mandiri (Persero) Tbk yang masing-masing menjabat sebagai *IT Security Lead Subsidiary IT Security Support* dan First Senior Manager UI/UX Designer. Teknik pemilihan partisipan menggunakan *purposive sampling*, yaitu pemilihan informan secara sengaja berdasarkan kriteria tertentu, yakni memiliki pengetahuan, pengalaman, dan keterlibatan langsung dalam pengelolaan sistem keamanan dan layanan digital perbankan (Huda, 2021). Teknik ini dipilih untuk memperoleh data yang mendalam dan relevan dengan fokus penelitian.

Pengumpulan data dalam penelitian ini dilakukan melalui dua metode utama, yaitu studi pustaka dan wawancara. Studi pustaka digunakan untuk memperoleh data sekunder yang meliputi bahan hukum primer, sekunder, dan tersier, seperti peraturan perundang-undangan, buku, jurnal ilmiah, serta sumber resmi lainnya yang berkaitan dengan perlindungan data dan kejahatan siber. Sementara itu, data primer diperoleh melalui wawancara semi-terstruktur dengan narasumber yang telah ditentukan, menggunakan pedoman wawancara sebagai instrumen penelitian. Wawancara ini bertujuan untuk menggali informasi secara mendalam mengenai praktik perlindungan data nasabah serta upaya penanggulangan kejahatan *phishing* di lingkungan perbankan.

Teknik analisis data dalam penelitian ini menggunakan metode analisis kualitatif. Data yang telah dikumpulkan, baik dari studi pustaka maupun wawancara, kemudian diolah melalui tahapan *editing*, *coding*, dan *systematizing* untuk memastikan data tersusun secara sistematis dan relevan. Selanjutnya, data dianalisis dengan cara menafsirkan dan mengaitkannya dengan teori-teori hukum serta ketentuan peraturan perundang-undangan yang berlaku. Analisis ini bertujuan untuk memberikan pemahaman yang mendalam mengenai efektivitas perlindungan hukum terhadap keamanan data nasabah serta

mengidentifikasi kelemahan dan solusi dalam menghadapi kejahatan *phishing* di sektor perbankan (Muhammad, 2004).

HASIL

Peran Bank Mandiri dalam Melindungi Keamanan Data Nasabah dari Kejahatan Phising

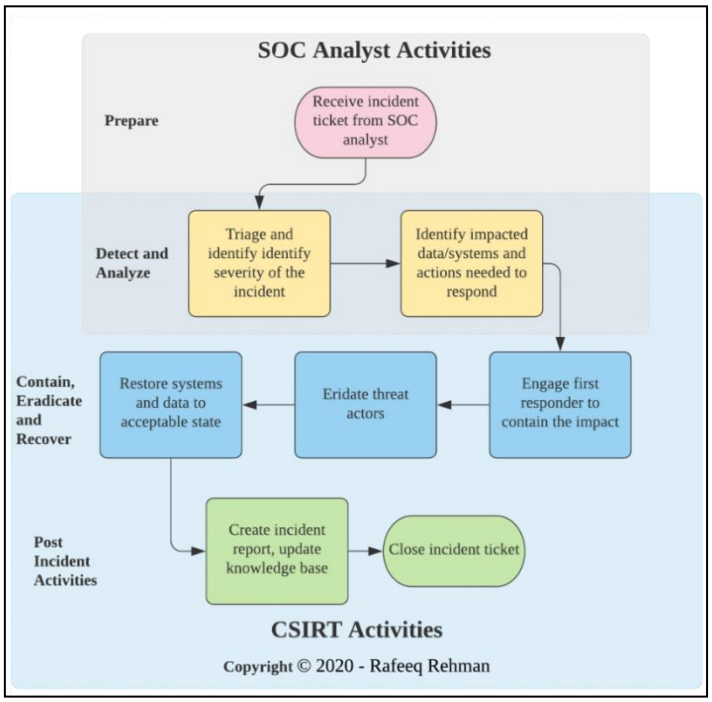
Penelitian ini menunjukkan bahwa Bank Mandiri menjalankan peran penting dalam melindungi keamanan data nasabah dari kejahatan phising melalui tiga bentuk peran, yaitu peran normatif, peran ideal, dan peran faktual. Bank Mandiri menjalankan peran normatif dengan mematuhi berbagai peraturan perundang-undangan, seperti Undang-Undang Perbankan dan Undang-Undang Perlindungan Data Pribadi, yang mewajibkan bank menjaga kerahasiaan data nasabah (Soekamto, 2005). Kepatuhan terhadap regulasi tersebut menjadi dasar dalam setiap aktivitas pengelolaan data, sehingga perlindungan terhadap data nasabah memiliki landasan hukum yang jelas dan mengikat.

Bank Mandiri menerapkan peran ideal dengan menggunakan berbagai teknologi keamanan dalam sistem perbankan digital. Sistem tersebut mencakup penggunaan *firewall* sebagai pengaman jaringan, *intrusion detection and prevention system (IDS/IPS)* untuk mendeteksi aktivitas mencurigakan, serta protokol keamanan *Secure Socket Layer/Transport Layer Security (SSL/TLS)* dalam proses transmisi data. Dalam era digital yang rentan terhadap ancaman siber, masyarakat mengharapkan bank memberikan perlindungan yang lebih dari sekadar kepatuhan normatif, termasuk edukasi yang berkelanjutan dan penerapan prinsip prudential principle sebagai bentuk kehati-hatian dalam menjaga kepentingan nasabah. (Dendhana, 2013) Bank Mandiri juga menerapkan sistem autentikasi berlapis melalui *Multi-Factor Authentication (MFA)* dan *One Time Password (OTP)* untuk memastikan bahwa akses terhadap akun nasabah hanya dilakukan oleh pihak yang berwenang. Sistem keamanan tersebut menunjukkan bahwa perlindungan data nasabah dilakukan secara teknis dan terstruktur.

Bank Mandiri melaksanakan peran faktual melalui kebijakan internal yang mendukung perlindungan data nasabah. Bank Mandiri menyusun Standar Operasional Prosedur (SOP) untuk penanganan insiden phising, membentuk *Computer Security Incident Response Team (CSIRT)*, serta menyelenggarakan pelatihan keamanan informasi bagi karyawan. Bank Mandiri juga memberikan edukasi kepada nasabah melalui program literasi digital untuk meningkatkan kesadaran terhadap risiko kejahatan phising (Chotimah, 2019). Pelaksanaan

kebijakan tersebut menunjukkan bahwa perlindungan data tidak hanya bergantung pada sistem teknologi, tetapi juga melibatkan sumber daya manusia.

Sebagai bentuk visualisasi dari temuan tersebut, sistem perlindungan data nasabah dapat dilihat pada Gambar 1 berikut.



Gambar 1. Sistem Perlindungan Keamanan Data Nasabah

Gambar tersebut menunjukkan bahwa sistem perlindungan keamanan menerapkan sistem perlindungan berlapis yang mencakup keamanan jaringan, autentikasi pengguna, serta mekanisme respons insiden. Setiap komponen dalam sistem tersebut memiliki fungsi yang saling mendukung dalam menjaga keamanan data nasabah.

Penelitian ini juga menemukan adanya kondisi yang menunjukkan keterbatasan dalam perlindungan data nasabah. Sebagian nasabah masih memiliki tingkat literasi digital yang rendah sehingga nasabah tersebut mudah memberikan informasi pribadi kepada pihak yang tidak berwenang. Perkembangan teknologi informasi juga menyebabkan metode kejahatan phising menjadi semakin kompleks dan sulit dideteksi oleh sistem keamanan yang ada. Kondisi tersebut menunjukkan bahwa perlindungan data nasabah masih menghadapi tantangan dari faktor eksternal.

Perlindungan Hukum terhadap Keamanan Data Nasabah Bank Mandiri dari Kejahatan Phising Berdasarkan Peraturan Perundang-Undangan di Indonesia

Penelitian ini menunjukkan bahwa perlindungan hukum terhadap keamanan data nasabah dari kejahatan phising dilakukan melalui perlindungan hukum preventif dan perlindungan hukum represif. Perlindungan hukum preventif bertujuan untuk mencegah terjadinya pelanggaran terhadap data nasabah. Bank Mandiri melaksanakan perlindungan preventif melalui penerapan sistem keamanan teknologi dan pemberian edukasi kepada nasabah. Pelaksanaan perlindungan tersebut didasarkan pada ketentuan dalam Undang-Undang Perbankan, Undang-Undang Perlindungan Konsumen, Undang-Undang Perlindungan Data Pribadi, serta Peraturan Otoritas Jasa Keuangan.

Ketentuan mengenai rahasia bank sebagai bentuk perlindungan hukum terhadap data pribadi nasabah tercantum dalam Pasal 40 Ayat (1) Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Dalam pasal tersebut disebutkan bahwa bank memiliki kewajiban untuk menjaga kerahasiaan informasi terkait nasabah penyimpan dan simpanannya. Namun, kewajiban ini dikecualikan dalam kondisi tertentu sebagaimana diatur dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 43, Pasal 44, dan Pasal 44A. Dengan demikian, informasi yang wajib dirahasiakan oleh pihak bank atau pihak terafiliasi terbatas pada data yang menyangkut nasabah penyimpan dan dana simpanannya (Rossana, 2016).

Pasal 65 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menegaskan larangan bagi setiap orang untuk secara melawan hukum memperoleh, mengumpulkan, mengungkapkan, atau menggunakan data pribadi milik orang lain. Larangan ini diberlakukan untuk mencegah tindakan yang dapat merugikan subjek data pribadi, baik karena penyalahgunaan maupun pemanfaatan tanpa dasar hukum yang sah. Ketentuan ini menempatkan data pribadi sebagai informasi yang harus dijaga kerahasiaan dan integritasnya.

Perlindungan hukum represif bertujuan untuk menindak pelaku kejahatan *phising* setelah terjadinya pelanggaran. Penanganan kejahatan *phising* dilakukan melalui proses pelaporan, investigasi, serta penindakan berdasarkan ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik dan Kitab Undang-Undang Hukum Pidana. Proses tersebut melibatkan berbagai lembaga, seperti Otoritas Jasa Keuangan, Badan Siber dan Sandi Negara, serta aparat penegak hukum. Mekanisme tersebut menunjukkan bahwa sistem hukum telah menyediakan sarana untuk memberikan perlindungan kepada nasabah.

Sebagai visualisasi dari kerangka perlindungan hukum tersebut, dapat dilihat pada Gambar 2 berikut.

Gambar 2. Kerangka Perlindungan Hukum terhadap Data Nasabah dari Kejahatan Phising

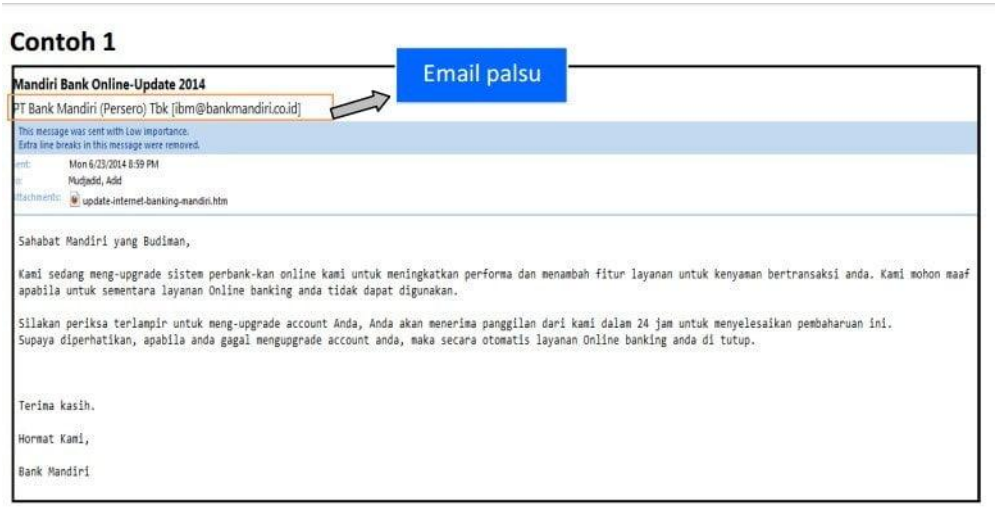
Gambar tersebut menunjukkan bahwa perlindungan hukum dilakukan melalui dua pendekatan utama, yaitu *preventive* dan *repressive*. Kedua pendekatan tersebut bekerja secara berkesinambungan dalam memberikan perlindungan terhadap data nasabah.

Penelitian ini juga menemukan adanya hambatan dalam pelaksanaan perlindungan hukum tersebut. Koordinasi antar lembaga yang terlibat dalam penanganan kejahatan siber belum berjalan secara optimal. Penegakan hukum terhadap pelaku kejahatan phising juga masih menghadapi kendala dalam praktik. Kondisi tersebut menunjukkan bahwa efektivitas perlindungan hukum masih memerlukan peningkatan.

Hambatan dalam Perlindungan Keamanan Data Nasabah dari Kejahatan Phising

Bank Mandiri sebagai salah satu bank terbesar di Indonesia memiliki tanggung jawab fundamental dalam melindungi data nasabah dari berbagai ancaman siber, termasuk kejahatan *phising*. Pencurian data dan serangan siber umumnya terjadi karena kelemahan dalam sistem keamanan. Berbagai faktor dapat membuat sistem keamanan tidak berjalan optimal, seperti keterbatasan sumber daya, kurangnya pengetahuan, serta kesalahan manusia. (Violita et al., 2025). Penelitian ini menunjukkan bahwa perlindungan keamanan data nasabah dari kejahatan phising masih menghadapi berbagai hambatan. Hambatan tersebut berasal dari faktor internal dan faktor eksternal. Faktor eksternal mencakup rendahnya tingkat literasi digital masyarakat serta perkembangan teknologi yang menyebabkan kejahatan phising semakin kompleks. Faktor internal mencakup keterbatasan dalam koordinasi antar lembaga

dalam menangani kejahatan siber. Bentuk kejahatan phising yang sering terjadi pada nasabah Bank Mandiri dapat dilihat pada Gambar 3.



Gambar 3. Bentuk Kejahatan Phising

Penelitian ini menunjukkan bahwa kejahatan phising terjadi dalam berbagai bentuk. Pelaku menggunakan email dan SMS untuk mengarahkan nasabah mengakses tautan berbahaya. Pelaku juga membuat website palsu yang menyerupai aplikasi Livin' by Mandiri untuk memperoleh data login nasabah. Pelaku menggunakan aplikasi pesan seperti WhatsApp dengan identitas visual Bank Mandiri untuk meyakinkan korban. Pelaku melakukan *social engineering* melalui telepon atau *vishing* dengan mengaku sebagai petugas bank. Pelaku juga menyebarkan aplikasi palsu melalui platform digital seperti Google Play Store untuk menipu nasabah.

Penelitian ini menunjukkan bahwa variasi bentuk kejahatan phising menjadi hambatan utama dalam perlindungan data nasabah. Sebagian nasabah tetap menjadi korban meskipun sistem keamanan telah diterapkan. Kondisi tersebut menunjukkan adanya kesenjangan antara sistem perlindungan yang tersedia dengan perilaku pengguna layanan perbankan digital.

PEMBAHASAN

Penelitian ini menunjukkan bahwa peran Bank Mandiri dalam melindungi keamanan data nasabah dari kejahatan phising merupakan aspek yang sangat krusial dalam era digitalisasi sektor perbankan. Perkembangan layanan *electronic banking (e-banking)* memberikan

kemudahan bagi masyarakat dalam melakukan transaksi keuangan, tetapi kondisi tersebut juga membuka peluang terjadinya kejahatan siber, khususnya phising yang bertujuan memperoleh data sensitif nasabah seperti PIN, OTP, dan kata sandi. Tingginya ancaman kejahatan phising menunjukkan bahwa perlindungan data nasabah menjadi tanggung jawab yang tidak hanya bersifat teknis, tetapi juga mencakup aspek normatif, ideal, dan faktual dalam praktiknya (Maramis, 2025).

Analisis hasil penelitian menunjukkan bahwa Bank Mandiri telah melaksanakan peran normatif sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Bank Mandiri memiliki kewajiban hukum untuk melindungi data nasabah sebagaimana diatur dalam Undang-Undang Perbankan, Undang-Undang Perlindungan Data Pribadi, serta Undang-Undang Informasi dan Transaksi Elektronik. Regulasi tersebut menegaskan bahwa data pribadi merupakan bagian dari hak yang harus dilindungi oleh negara dan lembaga keuangan. Bank Mandiri melaksanakan kewajiban tersebut melalui penerapan prinsip transparansi, akuntabilitas, serta pembatasan pengumpulan data sesuai kebutuhan layanan. Bank Mandiri juga memastikan adanya persetujuan eksplisit dari nasabah sebelum melakukan pemrosesan data serta memberikan hak akses dan koreksi kepada nasabah atas data yang dimiliki (Soekamto, 2005). Penerapan tersebut menunjukkan bahwa perlindungan data nasabah telah memiliki dasar hukum yang kuat dan menjadi bagian dari tanggung jawab institusional bank.

Analisis terhadap peran normatif juga menunjukkan bahwa Bank Mandiri melaksanakan kepatuhan terhadap standar keamanan sistem informasi yang ditetapkan oleh regulator, seperti Otoritas Jasa Keuangan dan Bank Indonesia. Bank Mandiri melakukan audit internal dan eksternal, pembaruan sistem keamanan, serta pelatihan kepatuhan bagi karyawan untuk memastikan bahwa operasional berjalan sesuai dengan ketentuan hukum. Pembentukan *Computer Security Incident Response Team (CSIRT)* menunjukkan bahwa bank memiliki mekanisme yang terstruktur dalam menangani risiko keamanan siber. Temuan tersebut menunjukkan bahwa peran normatif tidak hanya terbatas pada pemenuhan kewajiban hukum formal, tetapi juga mencerminkan tanggung jawab institusional dalam menjaga kepercayaan nasabah.

Analisis terhadap peran ideal menunjukkan bahwa Bank Mandiri menerapkan sistem keamanan yang bersifat preventif dan berlapis. Bank Mandiri menggunakan *firewall*, *intrusion detection system (IDS)*, *intrusion prevention system (IPS)*, serta protokol keamanan *Secure Socket*

Layer/Transport Layer Security (SSL/TLS) untuk melindungi sistem perbankan digital. Bank Mandiri juga menerapkan sistem autentikasi berlapis melalui *Multi-Factor Authentication (MFA)* dan *One Time Password (OTP)*. Pemanfaatan teknologi berbasis *Artificial Intelligence* dan *machine learning* memungkinkan bank mendeteksi pola ancaman secara *real-time* sehingga meningkatkan kemampuan pencegahan terhadap kejahatan phising. Temuan tersebut menunjukkan bahwa Bank Mandiri tidak hanya bersifat reaktif, tetapi juga proaktif dalam menghadapi ancaman siber yang terus berkembang.

Analisis terhadap peran faktual menunjukkan bahwa implementasi kebijakan internal menjadi faktor penting dalam mendukung efektivitas perlindungan data nasabah. Bank Mandiri menerapkan Standar Operasional Prosedur (SOP) dalam penanganan insiden phising, kebijakan keamanan informasi, serta prosedur verifikasi berlapis. Bank Mandiri juga menggunakan teknologi enkripsi untuk melindungi data yang disimpan maupun yang ditransmisikan. Selain itu, fitur keamanan seperti *One-Time Password (OTP)*, autentikasi biometrik, dan notifikasi transaksi secara *real-time* memberikan perlindungan tambahan terhadap akses tidak sah. Bank Mandiri juga melakukan evaluasi sistem keamanan melalui penilaian risiko, simulasi serangan, dan pengembangan sistem keamanan secara berkelanjutan. Upaya tersebut menunjukkan bahwa perlindungan data tidak hanya bergantung pada teknologi, tetapi juga pada kesiapan sistem dan sumber daya manusia (Chotimah, 2019).

Perbandingan dengan literatur menunjukkan bahwa hasil penelitian ini sejalan dengan teori peran yang dikemukakan oleh Soerjono Soekamto yang membagi peran menjadi peran normatif, ideal, dan faktual (Soekamto, 2005). Hasil penelitian ini juga sesuai dengan konsep perlindungan hukum yang membedakan perlindungan menjadi preventif dan represif. Perlindungan preventif terlihat dari penerapan sistem keamanan dan edukasi kepada nasabah, sedangkan perlindungan represif terlihat dari mekanisme penanganan kasus phising melalui pelaporan, investigasi, dan penindakan hukum. Penelitian ini memperkuat temuan sebelumnya yang menunjukkan bahwa perlindungan hukum tidak hanya bergantung pada regulasi, tetapi juga pada implementasi yang efektif di lapangan.

Implikasi temuan penelitian ini menunjukkan bahwa belum adanya undang-undang yang mengatur secara eksplisit mengatur *phising* di Indonesia. Maka dari itu, bank memiliki tanggung jawab dalam menyediakan sistem keamanan yang memadai dan melakukan pengawasan terhadap transaksi. Regulator memiliki peran dalam menetapkan dan mengawasi

kebijakan perlindungan data. Nasabah memiliki peran dalam menjaga kerahasiaan informasi pribadi dan meningkatkan kewaspadaan terhadap modus kejahatan siber. Temuan ini menunjukkan bahwa peningkatan literasi digital masyarakat menjadi faktor penting dalam mencegah kejahatan phising karena sebagian besar serangan memanfaatkan kelemahan pengguna.

Penelitian ini juga menunjukkan adanya keterbatasan dalam perlindungan data nasabah. Modus kejahatan phising berkembang secara cepat dan semakin kompleks sehingga sulit dideteksi oleh sistem keamanan yang ada. Rendahnya tingkat literasi digital masyarakat menyebabkan sebagian nasabah masih menjadi korban kejahatan phising. Keterbatasan kontrol terhadap platform eksternal seperti media sosial dan aplikasi pesan instan juga meningkatkan risiko terjadinya kejahatan phising. Koordinasi antar lembaga dalam penanganan kejahatan siber belum berjalan secara optimal sehingga mempengaruhi efektivitas penegakan hukum. Dari perspetif korban, dampak *phising* tidak hanya bersifat finansial tetapi juga psikologis. *Phising* menimbulkan dampak serius, seperti kerugian finansial, kerusakan reputasi, dan gangguan psikologis (Azura et al., 2025).

Keterbatasan penelitian ini terletak pada ruang lingkup penelitian yang hanya berfokus pada satu institusi perbankan, yaitu Bank Mandiri, sehingga hasil penelitian belum dapat digeneralisasi secara luas. Jumlah narasumber yang terbatas menyebabkan data empiris yang diperoleh belum sepenuhnya menggambarkan kondisi secara menyeluruh. Penelitian ini juga belum mengkaji secara mendalam aspek teknis sistem keamanan yang digunakan oleh bank. Penelitian selanjutnya dapat memperluas objek penelitian, menambah jumlah narasumber, serta mengkaji aspek teknologi secara lebih rinci agar diperoleh hasil yang lebih komprehensif.

KESIMPULAN

Berdasarkan pembahasan yang telah diuraikan, dapat disimpulkan bahwa peran Bank Mandiri dalam melindungi keamanan data nasabah dari kejahatan *phishing* telah dilaksanakan secara komprehensif melalui pendekatan normatif, ideal, dan faktual. Secara normatif, Bank Mandiri telah menjalankan kewajibannya sesuai dengan ketentuan peraturan perundang-undangan yang berlaku, termasuk penerapan prinsip kerahasiaan data, kehati-hatian, serta kepatuhan terhadap regulasi perlindungan data dan konsumen. Secara ideal, Bank Mandiri tidak hanya berfokus pada kepatuhan hukum, tetapi juga berupaya memenuhi ekspektasi

masyarakat melalui penerapan teknologi keamanan canggih, sistem deteksi dini, serta edukasi berkelanjutan kepada nasabah. Sementara itu, secara faktual, implementasi perlindungan dilakukan melalui kebijakan internal yang terstruktur, penggunaan teknologi enkripsi, autentikasi berlapis, serta mekanisme respons insiden yang cepat dan terkoordinasi. Meskipun demikian, tantangan seperti rendahnya literasi digital masyarakat, perkembangan modus *phishing* yang semakin canggih, serta keterbatasan pengawasan terhadap platform eksternal menunjukkan bahwa perlindungan data nasabah masih memerlukan peningkatan berkelanjutan.

Di sisi lain, perlindungan hukum terhadap keamanan data nasabah Bank Mandiri dari kejahatan *phishing* di Indonesia telah memiliki landasan yang kuat melalui berbagai peraturan perundang-undangan, baik dalam bentuk perlindungan preventif maupun represif. Perlindungan preventif diwujudkan melalui pengaturan kewajiban bank dalam menjaga keamanan data, memberikan edukasi, serta menerapkan sistem keamanan yang memadai, sebagaimana diatur dalam Undang-Undang Perbankan, Undang-Undang Perlindungan Konsumen, Undang-Undang Perlindungan Data Pribadi, serta regulasi OJK. Sementara itu, perlindungan represif diwujudkan melalui penegakan hukum terhadap pelaku kejahatan *phishing* berdasarkan ketentuan dalam UU ITE dan KUHP, serta mekanisme pemulihan hak-hak korban. Namun demikian, meskipun kerangka hukum yang ada telah cukup komprehensif, efektivitas implementasinya masih memerlukan penguatan, khususnya dalam aspek penegakan hukum, koordinasi antar lembaga, serta peningkatan kesadaran masyarakat. Dengan demikian, perlindungan data nasabah tidak hanya menjadi tanggung jawab bank, tetapi juga memerlukan sinergi antara pemerintah, aparat penegak hukum, pelaku industri, dan masyarakat secara luas.

Berdasarkan kesimpulan tersebut, disarankan agar Bank Mandiri terus meningkatkan sistem keamanan teknologi informasi dengan mengadopsi inovasi terbaru, seperti penguatan sistem berbasis *Artificial Intelligence*, pengembangan *zero trust architecture*, serta peningkatan kemampuan deteksi ancaman secara real-time. Selain itu, Bank Mandiri perlu memperluas program edukasi dan literasi digital kepada nasabah secara lebih masif dan tersegmentasi, khususnya bagi kelompok masyarakat yang memiliki tingkat literasi digital rendah. Pendekatan edukasi juga perlu dilakukan secara kolaboratif dengan lembaga pemerintah, institusi pendidikan, serta platform digital guna menciptakan kesadaran kolektif terhadap bahaya *phishing*. Di sisi internal, penguatan kapasitas sumber daya manusia melalui pelatihan

berkala serta peningkatan standar operasional prosedur juga menjadi langkah penting dalam meminimalisir risiko human error.

Selanjutnya, dari aspek regulasi dan penegakan hukum, pemerintah dan otoritas terkait perlu memperkuat pengawasan terhadap penyelenggara sistem elektronik serta meningkatkan efektivitas penindakan terhadap pelaku kejahatan siber. Diperlukan pula harmonisasi dan pembaruan regulasi yang lebih spesifik terkait kejahatan *phishing* agar memberikan kepastian hukum yang lebih jelas. Selain itu, peningkatan koordinasi antar lembaga seperti OJK, BSSN, dan aparat penegak hukum harus terus dioptimalkan untuk mempercepat penanganan kasus dan pemulihan kerugian korban. Bagi masyarakat atau nasabah, disarankan untuk lebih meningkatkan kewaspadaan dalam menggunakan layanan perbankan digital, tidak mudah memberikan data pribadi, serta selalu memverifikasi keaslian informasi yang diterima. Dengan adanya sinergi antara bank, regulator, dan masyarakat, diharapkan sistem perlindungan data nasabah dari kejahatan *phishing* dapat berjalan lebih efektif, adaptif, dan berkelanjutan di tengah perkembangan teknologi yang semakin pesat.

DAFTAR PUSTAKA

Alsayed, A. O., & Bilgrami, A. L. (2017). E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Emerging Technology and Advanced Engineering, 7*(1), 109–114. https://www.ijetae.com/files/Volume7Issue1/IJETAE_0117_19.pdf

Asril, J. (2018). Rahasia Bank dan Perkembangan Pengaturannya dalam Hukum Positif. *Jurnal Ilmiah Manajemen, Ekonomi, & Akuntansi (MEA), 2*(1), 237–250. https://doi.org/10.31955/mea.vol2.iss1.pp237-250

Azura, A. A., Monica, & Banke, R. (2025). Phishing sebagai Kejahatan Dunia Maya: Analisis Yuridis dan Upaya Pencegahannya. *Causa: Jurnal Hukum dan Kewarganegaraan, 11*(9), 21–30. https://doi.org/10.3783/causa.v11i9.12400

Balaka, K. I., Hakim, A. R., & Sulistyany, F. D. (2024). Pencurian Informasi Nasabah di Sektor Perbankan: Ancaman Serius di Era Digital. *Yustitiabelen, 10*(2), 105–130. https://doi.org/10.36563/yustitiabelen.v10i2.1167

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. *Jurnal Politica: Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, 10*(2), 113–128. https://doi.org/10.22212/jp.v10i2.1447

Dendhana, T. O. (2013). Penerapan Prudential Banking Principle dalam Upaya Perlindungan Hukum bagi Nasabah Penyimpan Dana. *Lex et Societatis, 1*(1), 116–121. https://doi.org/10.35796/les.v1i1.1303

Effendi, J., Ibrahim, J., & Rijadi, P. (2016). *Metode Penelitian Hukum: Normatif dan Empiris*. Kencana.

Hadjon, P. M. (1987). *Perlindungan Hukum bagi Rakyat Indonesia*. Bina Ilmu.

Huda, M. C. (2021). *Metode Penelitian Hukum (Pendekatan Yuridis Sosiologis)*. The Mahfud Ridwan Institute.

Kadarudin. (2021). *Penelitian di Bidang Ilmu Hukum (Sebuah Pemahaman Awal)*. Formaci.

Maramis, A. V. (2025). Tinjauan Yuridis terhadap Perlindungan Data Pribadi dalam Mengatasi Cybercrime pada Kasus Phishing. *Lex Privatum, 14*(5). https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/60333

Muhammad, A. (2004). *Hukum dan Penelitian Hukum*. Citra Aditya Bakti.

Rossana, G. (2016). Penafsiran Pasal 40 Undang-Undang Nomor 10 Tahun 1998 Mengenai Kerahasiaan Bank. *LamLaj, 1*(2), 119–128. https://doi.org/10.32801/lamlaj.v1i2.13

Soekanto, S. (2005). *Sosiologi: Suatu Pengantar*. Rajawali Press.

Wibowo, S. H., Wahyuddin, S., Permana, A. A., Sembiring, S., Wahidin, A. J., Nugroho, J. W., & Adhicandra, I. (2023). *Teknologi Digital di Era Modern*. Global Eksekutif Teknologi.

Yudha, F., & Panji, A. M. (2018). Perancangan Aplikasi Pengujian Celah Keamanan pada Aplikasi Berbasis Web. *Cyber Security dan Forensik Digital, 1*(1), 1–6. https://doi.org/10.14421/csecurity.2018.1.1.1216