Author's name: Danam Isyafara Bahapasca, Muhammad Rustamaji. (2025). Title: ANALISIS PERLINDUNGAN HUKUM DAN TANGGUNG JAWAB PERDATA BANK TERHADAP NASABAH KORBAN PHISHING BERDASARKAN UNDANG-UNDANG NO. 8 TAHUN 1999. *Verstek*, 13(3): 501-516. DOI: https://doi.org/10.20961/jv.v13i3.103869

Verstek Jurnal Hukum Acara

Volume 13 Issue 3, 2025
E-ISSN: 2355-0406

ANALISIS PERLINDUNGAN HUKUM DAN TANGGUNG JAWAB PERDATA BANK TERHADAP NASABAH KORBAN PHISHING BERDASARKAN UNDANG-UNDANG NO. 8 TAHUN 1999

Mohamad Sabiq Mohamad Nur*[1], Dara Pustika Sukma[2]
[1,2]Fakultas Hukum Ilmu Sosial dan Ilmu Politik,Universitas Terbuka
Email korespondensi: abisabiq020699@gmail.com

Abstrak: Latar belakang penelitian ini berkaitan dengan peningkatan pemanfaatan layanan perbankan elektronik yang seiring dengan meningkatnya ancaman kejahatan dunia maya, khususnya phishing, yang mengakibatkan kerugian finansial bagi nasabah dan merusak kepercayaan publik terhadap sistem perbankan digital. Penelitian ini bertujuan untuk menganalisis perlindungan hukum terhadap nasabah serta tanggung jawab perdata bank, serta mengidentifikasi upaya hukum yang dapat diakses oleh nasabah korban phishing berdasarkan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan peraturan dan konseptual. Hasil penelitian menunjukkan bahwa bank memiliki kewajiban hukum terkait jaminan keamanan sistem dan data, sesuai dengan Peraturan Otoritas Jasa Keuangan (OJK) dan undang-undang terkait. Tanggung jawab perdata bank dapat ditegakkan apabila terbukti ada kelalaian dalam menjalankan kewajiban tersebut. Nasabah korban phishing memiliki opsi hukum, termasuk pelaporan pidana dan litigasi perdata, namun Undang-Undang Perlindungan Konsumen memberikan jalur penyelesaian sengketa lebih terstruktur melalui pengaduan internal dan LAPS SJK. Kesimpulannya, meskipun ada kerangka hukum, perlindungan nasabah bergantung pada pembuktian dan optimalisasi mekanisme penyelesaian sengketa.

Kata kunci: Phishing, Perlindungan Hukum, Tanggung Jawab Perdata, Bank, LAPS SJK.

Abstract: *The background of this research is related to the increase in the use of electronic banking services in line with the increasing threat of cybercrime, especially phishing, which results in financial losses for customers and damages public trust in the digital banking system. This research aims to analyze legal protection for customers and bank civil liability, as well as identify legal remedies that can be accessed by customers who are victims of phishing based on Law Number 8 of 1999 concerning Consumer Protection. The method used is normative legal research with a regulatory and conceptual approach. The results of the study show that banks have legal obligations related to system and data security guarantees, in accordance with the Financial Services Authority (OJK) Regulation and related laws. The bank's civil liability can be enforced if it is proven that there is negligence in carrying out these obligations. Customers who are victims of phishing have legal options, including criminal reporting and civil litigation, but the Consumer Protection Law provides a more structured dispute resolution path through internal complaints and SJK LAPS. In conclusion, despite the existence of a legal framework, customer protection depends on proving and optimizing dispute resolution mechanisms.*

Keywords: *Phishing, Legal Protection, Civil Liability, Bank, LAPS SJK.*

1. Pendahuluan

Lembaga perbankan memainkan peran penting sebagai pilar fundamental dalam arsitektur ekonomi suatu negara, berfungsi sebagai perantara keuangan, agen kepercayaan, dan agen pembangunan (Manga & Dianti, 2023). Perbankan secara inheren berkontribusi pada stabilitas moneter dan percepatan pembangunan nasional dengan memobilisasi dana publik dan menyalurkannya kembali ke perekonomian melalui fasilitas kredit atau pembiayaan, di samping menyediakan berbagai layanan keuangan lainnya (Manangin, 2022). Bank yang sehat dan dapat dipercaya merupakan prasyarat penting untuk pertumbuhan aktivitas ekonomi dan peningkatan kesejahteraan masyarakat, sehingga memposisikan sektor ini secara strategis, memerlukan regulasi dan pengawasan hukum yang komprehensif (Sinaga & Maulisa, 2022).

Perkembangan eksponensial teknologi informasi telah mendorong transformasi mendasar dalam industri perbankan global, termasuk di Indonesia, mengantarkan era perbankan digital (Paminto et al., 2024). Layanan perbankan elektronik (e-banking), seperti Internet banking, mobile banking, dan transaksi melalui Automated Teller Machines (ATM), telah menjadi bagian integral dari lanskap layanan keuangan modern, menawarkan efisiensi operasional bagi bank serta kemudahan, kecepatan, dan kemudahan akses bagi nasabah (Oktana et al., 2023). Sambil menghasilkan banyak manfaat, digitalisasi ini secara bersamaan memperkenalkan risiko baru dan kompleks, terutama mengenai keamanan sistem dan data pelanggan dalam ekosistem siber yang dinamis dan seringkali rentan (Sihombing et al., 2024).

Dengan meluasnya adopsi layanan e-banking, ancaman kejahatan dunia maya yang menargetkan sektor perbankan dan kliennya telah muncul, dengan phishing menjadi salah satu bentuk yang paling meluas dan merugikan (Ismail et al., 2022). Phishing merupakan bentuk penipuan siber yang canggih di mana pelaku (phisher) menggunakan teknik rekayasa sosial untuk menipu korban agar membocorkan informasi pribadi yang sensitif, seperti nama pengguna, kata sandi, nomor kartu kredit, atau One-Time Password (OTP) (Juniamalia & Fadlian, 2023). Phisher biasanya menyamar sebagai entitas atau lembaga tepercaya, seperti bank itu sendiri, melalui komunikasi elektronik penipuan seperti email, teks Layanan Pesan Singkat (SMS), pesan instan (misalnya, WhatsApp), atau dengan membuat situs web palsu (pemalsuan web) yang dirancang dengan cermat agar menyerupai yang sah, sehingga menjerat korban (Banjarnahor & Priyana, 2022).

Skema phishing mengeksploitasi kerentanan psikologis dan keterbatasan pemahaman teknis dari pengguna layanan perbankan digital tertentu (Orji, 2019). Korban sering didorong untuk mengklik tautan berbahaya atau memasukkan kredensial mereka ke halaman web palsu dengan berbagai dalih, termasuk pembaruan sistem, verifikasi akun, penawaran hadiah menarik, atau bahkan peringatan keamanan palsu yang ironisnya dirancang untuk mencuri kredensial

keamanan korban (Damayanti & Priyono, 2022). Keberhasilan phishing tidak hanya bergantung pada kecanggihan teknis phisher dalam meniru entitas yang sah tetapi juga secara signifikan pada kelalaian korban atau kurangnya uji tuntas dalam memverifikasi keaslian komunikasi atau tautan yang diterima, menciptakan kerentanan keamanan yang signifikan di luar kendali langsung infrastruktur keamanan lembaga perbankan.

Phishing tidak hanya menyebabkan kerugian finansial bagi nasabah, tetapi juga mengancam kepercayaan publik terhadap keamanan perbankan digital (Putri & Sugiyono, 2024). Respons yang lemah dapat menimbulkan biaya sosial tinggi, mengganggu sistem pembayaran, serta menciptakan ketidakpastian hukum yang menghambat kemajuan teknologi keuangan (Hasanudin & Babussalam, 2024). Oleh karena itu, penanggulangan phishing menjadi isu krusial bagi nasabah, perbankan, regulator, dan stabilitas sistem keuangan nasional.

Phishing dalam perbankan melibatkan irisan Hukum Perbankan, Hukum Kejahatan Siber, dan Hukum Perlindungan Konsumen (Ekawati, 2018). UU No. 7 Tahun 1992 mengatur kewajiban kehati-hatian perbankan, termasuk layanan TI oleh OJK. UU No. 11 Tahun 2008 menyediakan kerangka hukum untuk kejahatan siber, sementara UU No. 8 Tahun 1999 melindungi hak konsumen atas keamanan, kemudahan, dan informasi akurat.

Masalah utama dalam kasus phishing adalah penentuan tanggung jawab hukum, khususnya tanggung jawab perdata atas kerugian finansial pelanggan. Hal ini menimbulkan perdebatan mengenai sejauh mana bank bertanggung jawab sebagai penyedia layanan e-banking, terutama jika terdapat kelalaian pelanggan dalam menjaga kerahasiaan data. Ambiguitas ini, ditambah kompleksitas pembuktian di ranah digital, menuntut kajian terhadap bentuk perlindungan hukum dan mekanisme penyelesaian sengketa yang efektif berdasarkan UU No. 8 Tahun 1999.

Dengan latar belakang yang kompleks ini, penelitian ini terutama bertujuan untuk menganalisis dua aspek penting secara mendalam. *Pertama*, studi ini berupaya menganalisis bentuk-bentuk perlindungan hukum dan konstruksi tanggung jawab perdata bank terhadap nasabah yang menjadi korban phishing dalam konteks pemanfaatan layanan e-banking. *Kedua*, penelitian ini berupaya untuk mengidentifikasi dan memeriksa berbagai upaya hukum hukum, baik litigasi maupun non-litigasi, yang tersedia bagi pelanggan yang telah menjadi korban phishing untuk penyelesaian kasus mereka dan pemulihan kerugian mereka, dengan fokus khusus pada kerangka hukum yang ditetapkan oleh Undang-Undang Nomor 8 Tahun 1999. Melalui analisis aspek-aspek tersebut, penelitian ini diantisipasi dapat berkontribusi secara konseptual untuk memajukan keilmuan hukum, memberikan panduan bagi praktisi hukum dan perbankan, serta meningkatkan kesadaran masyarakat yang lebih luas dan pemahaman hukum mengenai hak dan kewajiban ketika menghadapi ancaman phishing di era digital.

2. Metode

Penelitian ini merupakan penelitian hukum normatif berbasis pustaka (Qamar & Rezah, 2020), yang menelaah hukum sebagai norma positif melalui pendekatan statute dan konseptual. Pendekatan statute meninjau norma hukum dalam peraturan perundang-undangan terkait, sedangkan pendekatan konseptual menganalisis konsep-konsep hukum seperti perlindungan konsumen, tanggung jawab perdata, dan kejahatan siber. Data yang digunakan adalah data sekunder, terdiri dari materi hukum primer seperti KUH Perdata, UU No. 8 Tahun 1999, UU No. 11 Tahun 2008, UU No. 27 Tahun 2022, serta peraturan OJK; dan materi sekunder seperti buku, jurnal, dan doktrin ahli (Sampara & Husen, 2016). Analisis dilakukan secara kualitatif dengan teknik interpretasi gramatikal, sistematis, dan teleologis untuk memahami norma hukum serta menyusun argumen hukum terkait perlindungan pelanggan dari phishing (Irwansyah, 2020).

3. Pembahasan

Kerangka Hukum untuk Phishing Perbankan: Kewajiban Penting Bank dan Perlindungan Fundamental Pelanggan

Phishing yang menargetkan nasabah bank di Indonesia tidak hanya merupakan risiko teknologi, tetapi juga memenuhi unsur tindak pidana dalam kerangka hukum nasional sebagai kejahatan siber (Erdiyanto, 2023). Modus seperti penawaran palsu, informasi biaya transfer menyesatkan, atau tautan penggantian kartu ilegal bertujuan memperoleh akses tidak sah atau mencuri data rahasia nasabah (Yusuf et al., 2022). Perbuatan ini melanggar Pasal 30 UU No. 11 Tahun 2008 tentang akses ilegal ke sistem elektronik dan Pasal 28 ayat (1) UU No. 1 Tahun 2024 terkait penyebaran informasi menyesatkan yang merugikan konsumen. Pengenalan phishing sebagai pelanggaran hukum menjadi dasar penting untuk memahami hubungan hukum antara bank, nasabah, dan ancaman digital eksternal.

Ancaman phishing menuntut analisis hukum atas posisi dan kewajiban bank sebagai lembaga jasa keuangan yang tunduk pada prinsip kehati-hatian sebagaimana diatur dalam UU No. 7 Tahun 1992. Prinsip ini mewajibkan bank bertindak profesional dan bertanggung jawab demi melindungi nasabah dan menjaga stabilitas sistem keuangan. Dalam layanan berbasis teknologi, prinsip tersebut menuntut bank menyediakan sistem elektronik yang aman dan andal, serta menerapkan manajemen risiko yang efektif guna mengantisipasi ancaman siber seperti phishing. Kewajiban ini menjadi dasar standar hukum spesifik bagi perbankan digital.

Kewajiban bank terkait teknologi informasi dan manajemen risiko diatur dalam POJK, seperti POJK No. 11/POJK.03/2022 yang mewajibkan tata kelola TI, infrastruktur andal, dan

sistem keamanan informasi, termasuk otentikasi berlapis seperti OTP untuk transaksi berisiko tinggi. Selain itu, POJK No. 18/POJK.03/2016 mewajibkan bank mengelola risiko operasional, termasuk risiko kegagalan TI dan penipuan eksternal. Kepatuhan terhadap ketentuan ini merupakan kewajiban hukum bagi bank penyedia layanan e-banking.

Dimensi penting lainnya yang memperkuat kewajiban bank adalah melindungi data pribadi nasabah yang kini diatur secara komprehensif dalam Undang-Undang Nomor 27 Tahun 2022. Sebagai pengontrol data, bank memikul tanggung jawab hukum penuh untuk memastikan bahwa seluruh siklus hidup pemrosesan data pribadi pelanggan yang mencakup akuisisi, penyimpanan, pemanfaatan, dan penghancuran dilakukan secara sah, adil, transparan, dan, yang terpenting, aman. Undang-Undang Nomor 27 Tahun 2022 mengamanatkan agar bank menerapkan langkah-langkah keamanan teknis dan organisasi yang tepat sesuai dengan tingkat risiko yang terlibat untuk mencegah akses, pengungkapan, atau modifikasi data pribadi yang tidak sah, termasuk data kredensial perbankan yang terutama menjadi sasaran serangan phishing. Kewajiban untuk melindungi kerahasiaan dan integritas data pribadi ini berkorelasi langsung dengan upaya pencegahan phishing karena keberhasilan phishing sering bergantung pada kemampuan phisher untuk memperoleh data pelanggan sensitif yang wajib dilindungi oleh bank.

Kewajiban bank tidak hanya mencakup aspek teknis, tetapi juga penyampaian informasi dan edukasi kepada nasabah. UU No. 8 Tahun 1999 dan POJK No. 22 Tahun 2023 mewajibkan bank memberi informasi yang akurat dan jujur, termasuk soal risiko. Dalam konteks phishing, ini mencakup edukasi proaktif tentang hak konsumen, risiko keamanan siber, serta imbauan untuk tidak membagikan data pribadi dan hanya bertransaksi melalui platform resmi.

Sebaliknya, di sisi lain spektrum hukum ini, nasabah, sebagai konsumen jasa keuangan, diberkahi dengan hak-hak dasar yang dijamin berdasarkan Pasal 4 Undang-Undang Nomor 8 Tahun 1999. Hak yang paling relevan untuk menghadapi ancaman phishing termasuk hak atas kenyamanan, keamanan, dan keselamatan dalam mengonsumsi barang dan/atau jasa; hak atas informasi yang akurat, jelas, dan jujur; dan hak untuk mendengarkan pendapat dan keluhan mereka. Hak atas keamanan dan keselamatan secara implisit mensyaratkan bahwa nasabah berhak mengharapkan tingkat perlindungan yang wajar yang diberikan oleh sistem bank terhadap ancaman yang dapat diperkirakan (Ferdiansyah et al., 2024). Selain itu, hak atas informasi menggarisbawahi hak nasabah atas penjelasan yang memadai mengenai pengoperasian layanan yang aman dan potensi risiko yang menyertainya, membentuk dasar bagi bank untuk memberikan pendidikan yang efektif. Mengakui hak-hak dasar pelanggan ini melengkapi penggambaran kerangka hukum yang mengatur hubungan bank-pelanggan dalam

konteks layanan digital.

Singkatnya, memeriksa kerangka hukum seputar phishing perbankan di Indonesia mengungkapkan struktur normatif yang cukup komprehensif yang menetapkan standar kewajiban yang signifikan bagi bank sekaligus memberikan perlindungan mendasar kepada nasabah (Sari & Sutabri, 2023). Bank, berpedoman pada prinsip kehati-hatian dan amanat khusus dari Peraturan Otoritas Jasa Keuangan dan Undang-Undang Nomor 27 Tahun 2022, memiliki kewajiban hukum yang penting untuk menyediakan sistem e-banking yang aman, mengelola risiko teknologi informasi secara hati-hati, menjaga data pribadi, serta memberikan informasi dan edukasi yang memadai. Bersamaan dengan itu, nasabah, sebagai konsumen, dilindungi oleh Undang-Undang Nomor 8 Tahun 1999, yang menjamin hak dasar mereka atas keselamatan, keamanan, informasi, dan pelayanan yang layak. Pemahaman tentang keseimbangan antara kewajiban bank dan hak nasabah ini merupakan landasan normatif yang penting untuk analisis selanjutnya mengenai tanggung jawab perdata bank jika terjadi insiden phishing yang mengakibatkan kerugian nasabah.

Analisis Tanggung Jawab Perdata Bank dalam Insiden Phishing

Ketika nasabah menderita kerugian akibat phishing yang mengeksploitasi layanan perbankan elektronik (Suhyana et al., 2021), fokus hukum perdata beralih ke tanggung jawab bank, meskipun tindakan kriminal dilakukan oleh phisher. Analisis tanggung jawab perdata bank ini kompleks, mengingat interaksi antara tindakan phisher, sistem keamanan bank, dan kelalaian nasabah. KUHPerdata, khususnya Pasal 1365, memberikan dasar hukum untuk menilai tanggung jawab bank, melalui doktrin perbuatan melawan hukum dan potensi wanprestasi berdasarkan hubungan kontraktual antara bank dan nasabah.

Penetapan tanggung jawab bank menurut Pasal 1365 KUH Perdata mensyaratkan pembuktian tindakan melawan hukum, kesalahan, kerugian, dan hubungan kausal. Dalam kasus phishing, pelanggaran dapat berupa kegagalan bank memenuhi kewajiban hukum, seperti tidak menerapkan standar keamanan TI (POJK), lalai melindungi data pribadi (UU No. 27/2022), atau tidak memberikan edukasi terkait risiko phishing (UU No. 8/1999). Kegagalan ini mencerminkan pelanggaran terhadap kewajiban hukum dan prinsip kehati-hatian yang melekat dalam industri perbankan.

Unsur kesalahan (schuld) yang dapat dikaitkan dengan bank, sering kali berupa kelalaian (culpa), sebagaimana diatur dalam Pasal 1366 KUHPerdata, harus ditetapkan. Kelalaian bank dapat terlihat dari kekurangan dalam desain sistem keamanan e-banking, kegagalan mendeteksi transaksi anomali, kurangnya pemantauan ancaman siber, atau tanggapan yang terlambat terhadap insiden keamanan. Penilaian kelalaian ini dilakukan dengan membandingkan tindakan

bank dengan standar perilaku yang diharapkan dari lembaga perbankan yang profesional dalam mengelola risiko digital. Menetapkan kelalaian ini memberikan dasar yang kuat untuk menegaskan tanggung jawab bank (Davis & Grayson, 2022).

Membuktikan unsur kerugian (*schade*) dalam kasus phishing biasanya mudah, umumnya bermanifestasi sebagai menipisnya dana dari akun pelanggan. Tantangan pembuktian yang lebih substansial sering muncul mengenai unsur kausalitas (*causaal verband*) antara kesalahan atau kelalaian bank dan kerugian yang diderita oleh nasabah. Bank mungkin berpendapat bahwa penyebab terdekat dari kerugian terletak semata-mata pada tindakan penipuan phisher dan / atau kerentanan pelanggan terhadap penipuan. Meskipun demikian, dari sudut pandang hukum, argumen kausalitas dapat ditetapkan dengan menunjukkan bahwa kelalaian bank misalnya, dalam bentuk sistem keamanan yang lemah atau pendidikan minimal menciptakan kondisi atau kerentanan yang secara signifikan memfasilitasi keberhasilan serangan phishing atau memperburuk kerugian yang dihasilkan. Dasar klaim ganti rugi mendapat dukungan eksplisit dalam ketentuan Pasal 58 Undang-Undang Nomor 27 Tahun 2022, yang memberikan hak kepada subjek data yang dirugikan oleh pelanggaran perlindungan data pribadi untuk meminta ganti rugi. Hal ini semakin menggarisbawahi konsekuensi perdata yang berasal dari kegagalan bank untuk melindungi data nasabah dalam konteks tindakan yang melanggar hukum sesuai dengan Pasal 1365 KUH Perdata (Shapiro, 2023).

Atau, tanggung jawab bank dapat dibangun untuk pelanggaran kontrak (gagal bayar). Hubungan hukum antara bank dan pelanggannya pada dasarnya bersifat kontraktual, mencakup perjanjian pembukaan rekening dan syarat dan ketentuan yang mengatur penggunaan layanan e-banking. Dalam perjanjian ini, bank memikul kewajiban kontraktual, baik yang dinyatakan secara eksplisit maupun tersirat oleh sifat layanan, untuk menyediakan layanan perbankan dengan aman dan andal. Kegagalan bank untuk memberikan tingkat keamanan sistem yang sesuai dengan standar industri, atau yang dapat diharapkan pelanggan secara wajar, sehingga memungkinkan kompromi akun melalui phishing, secara logis dapat dianggap sebagai pelanggaran kewajiban kontraktual ini (Irmawati et al., 2024). Berdasarkan prinsip-prinsip hukum kontrak, pihak yang melanggar berkewajiban untuk memberi kompensasi kepada pihak yang dirugikan atas kerugian yang diakibatkan oleh wanprestasi.

Setiap analisis tanggung jawab bank, baik terkait wanprestasi atau pelanggaran kontrak, harus mempertimbangkan perilaku pelanggan. Dalam banyak kasus, bank mengajukan argumen kelalaian kontributif, menyatakan bahwa nasabah berkontribusi pada kerugian dengan mengabaikan peringatan keamanan, mengklik tautan phishing, atau membocorkan kredensial kepada pihak ketiga. Argumen ini berlandaskan prinsip hukum perdata dan menjadi faktor

penting dalam menentukan kewajiban bank. Jika kelalaian ditemukan pada kedua belah pihak, prinsip pembagian tanggung jawab atau pengurangan kerusakan dapat diterapkan sesuai dengan tingkat kesalahan masing-masing pihak (Grimes, 2024).

Kesimpulannya, tanggung jawab perdata bank setelah insiden phishing tidak otomatis. Namun, ada dasar hukum yang kuat untuk menetapkan tanggung jawab tersebut, terutama melalui mekanisme wanprestasi (tindakan yang melanggar hukum) atau pelanggaran kontrak. Penentuan tanggung jawab bank bergantung pada pembuktian kegagalan bank untuk memenuhi kewajiban hukumnya terkait keamanan sistem, perlindungan data, dan edukasi nasabah (sebagaimana diatur dalam Peraturan Otoritas Jasa Keuangan, Undang-Undang Nomor 27 Tahun 2022, dan Undang-Undang Nomor 8 Tahun 1999) kegagalan yang mungkin merupakan tindakan yang melanggar hukum atau pelanggaran kontrak yang melibatkan kesalahan atau kelalaian dan menunjukkan hubungan kausal dengan kerugian nasabah. Namun demikian, unsur kelalaian kontributif pelanggan tetap menjadi faktor kritis, selalu dipertimbangkan selama penyelesaian sengketa, membuat penentuan akhir kewajiban bank sangat bergantung pada analisis fakta yang cermat dan penerapan prinsip-prinsip hukum yang adil dalam setiap kasus. **Mekanisme Penyelesaian Sengketa dan Upaya Hukum untuk Korban Phishing**

Nasabah yang mengalami kerugian akibat phishing berhak mengupayakan berbagai upaya hukum. Upaya hukum ini adalah prosedur yang disediakan oleh sistem hukum untuk mencari keadilan dan melindungi hak (Gadjong, 2023). Dalam kasus phishing perbankan, nasabah memiliki beberapa alternatif jalur hukum, termasuk hukum pidana terhadap phisher, hukum perdata melalui litigasi di pengadilan, serta penyelesaian sengketa konsumen yang diatur dalam Undang-Undang Nomor 8 Tahun 1999 dan peraturan terkait jasa keuangan. Pemilihan jalur hukum yang tepat memerlukan pemahaman mendalam tentang karakteristik, tujuan, prosedur, dan hasil masing-masing opsi.

Tindakan awal yang dapat diambil adalah melaporkan insiden phishing kepada aparat penegak hukum, yaitu Kepolisian Negara Republik Indonesia, dengan dasar hukum dari Undang-Undang Nomor 11 Tahun 2008 tentang tindak pidana akses tidak sah, manipulasi informasi elektronik, atau penipuan elektronik; Pasal 378 KUHP tentang penipuan; dan Undang-Undang Nomor 8 Tahun 2010 tentang pencucian uang jika ada hasil yang disembunyikan. Tujuan utama dari jalur pidana adalah untuk menangkap dan menuntut phisher, meskipun proses ini tidak secara langsung menjamin pemulihan kerugian finansial pelanggan, kecuali melalui mekanisme restitusi yang penerapannya mungkin terbatas (Supriadi & Andarsyah, 2023).

Secara terpisah atau bersamaan dengan proses pidana terhadap phisher, nasabah dapat

mengupayakan upaya hukum perdata untuk mencari kompensasi atas kerugian yang ditimbulkan, terutama jika ada alasan untuk menegaskan tanggung jawab terhadap bank. Nasabah berhak untuk mengajukan gugatan perdata terhadap bank di Pengadilan Negeri yang berwenang, mendasarkan klaim mereka pada dugaan perbuatan melawan hukum (wanprestasi) atau pelanggaran kontrak, sesuai dengan analisis sebelumnya. Jalan litigasi ini merupakan mekanisme penyelesaian sengketa formal yang menghasilkan putusan yang mengikat secara hukum (Situmeang, 2021). Namun, litigasi dalam sistem pengadilan umum sering kali memerlukan garis waktu yang berlarut-larut dan biaya yang besar dan membebankan beban pembuktian yang cukup besar kepada pelanggan untuk membujuk pengadilan mengenai kesalahan atau kelalaian bank dan hubungan sebab-akibatnya dengan kerugian yang berasal dari insiden phishing.

Menyadari keterbatasan litigasi konvensional, hukum perlindungan konsumen Indonesia menyediakan mekanisme penyelesaian sengketa alternatif (ADR) yang lebih efisien, termasuk bagi nasabah bank. Langkah pertama dalam kerangka ini adalah pemanfaatan mekanisme Internal Dispute Resolution (IDR), yang diwajibkan oleh Undang-Undang Nomor 8 Tahun 1999 dan Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023. Nasabah yang dirugikan harus mengajukan keluhan secara tertulis atau lisan ke unit pengaduan yang ditunjuk bank. Mekanisme ini mewajibkan bank untuk menerima, mencatat, meninjau pengaduan, dan memberikan tanggapan dalam jangka waktu yang ditentukan. Tujuan tahap ini adalah untuk mendorong dialog dan penyelesaian damai antara nasabah dan bank.

Jika keluhan nasabah tidak mendapatkan tanggapan atau penyelesaian yang memadai dari bank dalam waktu yang ditentukan, atau jika kesepakatan tidak tercapai, penyelesaian sengketa eksternal (EDR) melalui lembaga khusus tersedia (Sirait et al., 2025). Lembaga yang berwenang dalam bidang jasa keuangan adalah Lembaga Alternatif Penyelesaian Sengketa di Bidang Jasa Keuangan (LAPS SJK), yang diatur dalam Peraturan Otoritas Jasa Keuangan Nomor 61/POJK.07/2020 dan berlandaskan pada prinsip Undang-Undang Nomor 8 Tahun 1999. LAPS SJK menawarkan mediasi, ajudikasi, atau arbitrase sebagai metode penyelesaian sengketa. Nasabah dapat mengajukan permohonan ke LAPS SJK setelah proses pengaduan internal gagal. Prosedur ini umumnya lebih cepat, lebih murah, dan lebih sederhana dibandingkan dengan litigasi di pengadilan.

Selanjutnya, Badan Penyelesaian Sengketa Konsumen yang operasinya diatur dalam Peraturan Menteri Nomor 72 Tahun 2020 umumnya memiliki kewenangan yang sama untuk menyelesaikan sengketa konsumen di berbagai sektor, meskipun LAPS SJK saat ini menjadi wadah utama sektor jasa keuangan. Penting untuk ditekankan bahwa semua jalan ini—baik

litigasi perdata atau mekanisme perlindungan konsumen pada dasarnya ditujukan untuk mewujudkan hak dasar konsumen atas ganti rugi, ganti rugi, dan/atau restitusi, sebagaimana dijamin dalam Pasal 4 huruf (h) Undang-Undang Nomor 8 Tahun 1999, jika kerugian terbukti timbul dari kesalahan atau kelalaian pelaku usaha (dalam konteks ini, bank, jika kewajibannya ditetapkan). Mekanisme penyelesaian sengketa konsumen ini dirancang untuk menawarkan pelanggan jalur yang lebih efektif untuk menegaskan hak mereka atas pemulihan kerugian.

Oleh karena itu, nasabah yang menjadi korban phishing perbankan memiliki beberapa opsi hukum yang dapat ditempuh secara serentak atau berurutan. Melaporkan insiden tersebut sebagai tindak pidana terutama menargetkan penuntutan dan hukuman terhadap phisher, sedangkan memulai gugatan perdata di pengadilan negeri memberikan mekanisme litigasi formal untuk mencari ganti rugi dari bank. Namun, kerangka hukum perlindungan konsumen menghadirkan jalur penyelesaian sengketa yang lebih terstruktur dan berpotensi lebih efisien, mulai dari mekanisme pengaduan internal wajib bank, yang dapat dilanjutkan ke forum alternatif seperti LAPS SJK. Pemahaman yang komprehensif tentang karakteristik, prosedur, kelebihan, dan kerugian setiap jalan sangat penting, memungkinkan pelanggan untuk memilih dan memanfaatkan upaya hukum yang paling sesuai untuk melindungi hak-hak mereka dan mengejar pemulihan optimal atas kerugian mereka saat menghadapi konsekuensi merugikan dari phishing.

4. KESIMPULAN DAN SARAN

Berdasarkan analisis dan diskusi sebelumnya, disimpulkan bahwa kerangka hukum Indonesia memberikan landasan normatif yang relatif komprehensif untuk melindungi nasabah bank dari phishing dan menentukan tanggung jawab bank. Perlindungan hukum bagi nasabah tidak hanya berasal dari hak-hak dasar yang dijamin oleh Undang-Undang Nomor 8 Tahun 1999, seperti hak atas keamanan dan informasi, tetapi juga didukung oleh kewajiban khusus yang dikenakan pada bank sebagai penyedia sistem elektronik dan pengendali data pribadi. Tugas-tugas tersebut mencakup penerapan standar keamanan teknologi informasi yang prudent sebagaimana diamanatkan oleh Peraturan Otoritas Jasa Keuangan, serta kewajiban pengamanan data pribadi nasabah berdasarkan Undang-Undang Nomor 27 Tahun 2022. Konsekuensi logis dari arsitektur normatif ini adalah bahwa tanggung jawab perdata bank atas kerugian nasabah yang timbul dari phishing dapat ditetapkan, terutama atas dasar tindakan yang melanggar hukum (tort), asalkan terbukti bahwa bank gagal melaksanakan kewajiban hukum ini, sehingga menunjukkan kesalahan atau kelalaian. Meskipun demikian, menegakkan tanggung jawab tersebut dalam perselisihan individu menghadirkan kerumitan, terutama mengenai bukti

kausalitas dan menilai kelalaian kontribusi pelanggan faktor-faktor yang sering menjadi penting dalam penyelesaian kasus.

Lebih lanjut disimpulkan bahwa pelanggan yang menjadi korban phishing memiliki akses ke berbagai mekanisme penyelesaian sengketa dan upaya hukum untuk pemulihan kerugian, di mana kerangka hukum perlindungan konsumen menyediakan jalur yang lebih terstruktur dan berorientasi pada pemberdayaan konsumen. Selain melaporkan tindakan pidana phisher kepada penegak hukum dan mengejar litigasi perdata umum terhadap bank di pengadilan distrik, sistem hukum menawarkan proses penyelesaian sengketa konsumen yang lebih mudah diakses. Proses ini diawali dengan mekanisme wajib penanganan pengaduan internal di lingkungan bank, sebagaimana diatur dalam Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023. Jika penyelesaian terbukti sulit dipahami pada tahap internal ini, nasabah dapat mengeskalasi kasus mereka ke LAPS SJK, lembaga independen yang menyediakan layanan mediasi, ajudikasi, atau arbitrase, yang diantisipasi dapat menawarkan efisiensi dan efektivitas yang lebih besar untuk menyelesaikan sengketa dalam sektor jasa keuangan. LAPS SJK yang berfungsi di bawah naungan Undang-Undang Nomor 8 Tahun 1999 berfungsi sebagai instrumen sentral yang memungkinkan nasabah untuk mewujudkan hak atas ganti rugi atau ganti rugi atas kerugian yang timbul akibat insiden phishing, terutama jika tanggung jawab bank dapat ditetapkan.

Mengikuti kesimpulan tersebut, beberapa saran diajukan untuk memperkuat perlindungan pelanggan dan meningkatkan kepastian hukum dalam mengelola insiden phishing perbankan. *Pertama*, lembaga perbankan disarankan untuk fokus mematuhi standar keamanan minimum yang diamanatkan oleh regulator dan secara proaktif dan terus berinvestasi dalam teknologi keamanan siber canggih dan sistem deteksi penipuan yang lebih canggih. Selain itu, literasi digital dan program pendidikan untuk pelanggan harus dirancang dengan inovasi yang lebih besar, keberlanjutan, dan efektivitas yang terukur dalam meningkatkan kewaspadaan terhadap taktik phishing yang terus berkembang. Ini berfungsi sebagai komponen penting untuk mengurangi risiko yang melekat dan potensi gugatan balik dari kelalaian kontributif. Memperkuat mekanisme penanganan keluhan internal yang ditandai dengan transparansi dan pendekatan berorientasi solusi sangat penting untuk membangun kembali kepercayaan pelanggan.

Kedua, direkomendasikan agar Otoritas Jasa Keuangan, dalam kapasitas pengaturannya, terus mengintensifkan pengawasannya terhadap kepatuhan bank terhadap penerapan Peraturan Otoritas Jasa Keuangan terkait mengenai keamanan teknologi informasi, manajemen risiko, perlindungan data pribadi, dan perlindungan konsumen. Mengakui kompleksitas yang melekat dalam menentukan tanggung jawab dalam kasus phishing, Otoritas Jasa Keuangan dapat

mempertimbangkan untuk mengeluarkan pedoman yang lebih rinci yang mengklarifikasi prinsip atau faktor yang mengatur alokasi kewajiban atas kerugian antara bank dan nasabah, terutama ketika masalah kelalaian kontributif muncul. Ini akan mendorong konsistensi yang lebih besar dalam praktik penyelesaian sengketa. Selain itu, promosi, peningkatan kapasitas, dan penjangkauan layanan LAPS SJK sebagai forum penyelesaian sengketa konsumen yang kredibel memerlukan peningkatan berkelanjutan.

Ketiga, sangat penting bagi nasabah perbankan untuk terus meningkatkan kesadaran terkait risiko phishing dan berhati-hati saat melakukan transaksi online dan menjaga data pribadi. Selain itu, nasabah harus diberdayakan dengan pengetahuan mengenai hak-hak hukumnya sebagai konsumen dan memiliki pemahaman dan kepercayaan diri untuk memanfaatkan prosedur pengaduan internal bank dan mekanisme penyelesaian sengketa eksternal melalui LAPS SJK jika mengalami kerugian akibat phishing. Akhirnya, bagi komunitas akademik dan peneliti masa depan, ada ruang lingkup yang cukup untuk penelitian lebih lanjut tentang efektivitas empiris LAPS SJK dalam menyelesaikan sengketa terkait phishing, analisis yang lebih dalam tentang yurisprudensi pengadilan mengenai pembagian tanggung jawab dalam kasus-kasus yang melibatkan kelalaian kontributif, dan pemeriksaan dampak teknologi baru (seperti Kecerdasan Buatan - AI) pada metodologi phishing dan implikasi hukum yang menyertainya.

Referensi

Banjarnahor, A. C., & Priyana, P. (2022). Analisis Yuridis Cybercrime terhadap Penanganan Kasus Phising Kredivo. *Hermeneutika: Jurnal Ilmu Hukum, 6*(1), 32- 36. https://doi.org/10.33603/hermeneutika.v6i1.6754

Colonial Regulations, *Staatsblad* Number 23 of 1847 on the *Burgerlijk Wetboek voor Indonesie*/the Civil Code. https://jdih.mahkamahagung.go.id/legal-product/ kitab- undang-undang-hukum-perdata/detail

Damayanti, M., & Priyono, E. A. (2022). Legal Consequences for LDMO Disclosing Personal Data of Transacting Parties: A Study of Legal Protection. *SIGn Jurnal Hukum, 4*(2), 221-232. https://doi.org/10.37276/sjh.v4i2.217

Davis, J. R., & Grayson, M. D. (2022). *Phishing: Identifying and Preventing Fraudulent Activities in the Digital World*. CyberSec Publishing.

Ekawati, D. (2018). Perlindungan Hukum terhadap Nasabah Bank yang Dirugikan Akibat Kejahatan Skimming Ditinjau dari Perspektif Teknologi Informasi dan Perbankan. *Unes Law Review, 1*(2), 157-171. https://doi.org/10.31933/law.v1i2.24

Erdiyanto, R. P. (2023). Penipuan Mengatasnamakan Bank Berbentuk Phising. *Jurnal Inovasi Global, 1*(2), 71-79. https://doi.org/10.58344/jig.v1i2.11

Ferdiansyah, D. S., Ameeralia, N. V., Putri, A. A. K., & Fikrie, S. N. (2024). Peran OJK dalam Perlindungan Konsumen terhadap Kebocoran Data pada Konsumen Jasa Keuangan Indonesia. *Media Hukum Indonesia, 2*(3), 301-305. Retrieved from https://ojs.daarulhuda.or.id/index.php/MHI/article/view/482

Gadjong, A. A. (2023). The Agreement of Personal Shopping Service through E-Commerce Platforms: A Case Study of Consumer Protection. *SIGn Jurnal Hukum, 4*(2), 388-401. https://doi.org/10.37276/sjh.v4i2.230

Government Regulation in Lieu of Law of the Republic of Indonesia Number 2 of 2022 on Job Creation (State Gazette of the Republic of Indonesia of 2022 Number 238, Supplement to the State Gazette of the Republic of Indonesia Number 6841). https://peraturan.go.id/id/perppu-no-2-tahun-2022

Grimes, R. A. (2024). *Fighting Phishing*. Wiley.

Hasanudin, A. F., & Babussalam, A. B. (2024). Perlindungan Hukum bagi Korban Kejahatan Phising yang Menguras Saldo M-Banking. *Jurnal Gagasan Hukum, 6*(1), 16-29. https://doi.org/10.31849/jgh.v6i01.18827

Irmawati, E., Pieries, J., & Widiarty, W. S. (2024). Perlindungan Hukum atas Data Pribadi Nasabah Bank Pengguna Mobile Banking dalam Perspektif UU No 27 Tahun 2022 tentang Kebocoran Data. *Jurnal Syntax Admiration, 5*(1), 12-27. https://doi.org/10.46799/jsa.v5i1.964

Irwansyah. (2020). *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*. Mirra Buana Media.

Ismail, N., Ramlee, Z., & Abas, A. (2022). The Legal Proof of Macau Scam in Malaysia. *Malaysian Journal of Syariah and Law, 10*(1), 23-33. https://doi.org/10.33102/mjsl.vol10no1.307

Juniamalia, A., & Fadlian, A. (2023). Perspektif Undang-Undang Tentang Informasi dan Transaksi Elektronik terhadap Cyber Crime dalam Bentuk Phising. *De Juncto Delicti: Journal of Law, 3*(1), 30-46. https://doi.org/10.35706/djd.v3i1.7985

Law of the Republic of Indonesia Number 1 of 1946 on the Penal Code Regulations. https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/814

Law of the Republic of Indonesia Number 1 of 1960 on Amendment of the Penal Code (State Gazette of the Republic of Indonesia of 1960 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 1921). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1357

Law of the Republic of Indonesia Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2024 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 6905). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1842

Law of the Republic of Indonesia Number 10 of 1998 on Amendment to Law Number 7 of 1992 on Banking (State Gazette of the Republic of Indonesia of 1998 Number 182, Supplement to the State Gazette of the Republic of Indonesia Number 3790). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/468

Law of the Republic of Indonesia Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/138

Law of the Republic of Indonesia Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952). https://www.dpr.go.id/dokumen/jdih/undang- undang/detail/1683 Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection (State Gazette of the Republic of Indonesia of 2022 Number 196, Supplement to the State Gazette of the Republic of Indonesia Number 6820). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1814

Law of the Republic of Indonesia Number 6 of 2023 on Enactment of Government Regulation in Lieu of Law Number 2 of 2022 on Job Creation Into Law (State Gazette of the Republic of Indonesia of 2023 Number 41, Supplement to the State Gazette of the Republic of Indonesia Number 6856). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1825

Law of the Republic of Indonesia Number 7 of 1992 on Banking (State Gazette of the Republic of Indonesia of 1992 Number 31, Supplement to the State Gazette of the Republic of Indonesia Number 3472). https://www.dpr.go.id/dokumen/jdih/undang- undang/detail/622

Law of the Republic of Indonesia Number 8 of 1999 on Consumer Protection (State Gazette of the Republic of Indonesia of 1999 Number 22, Supplement to the State Gazette of the Republic of Indonesia Number 3821). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/409

Law of the Republic of Indonesia Number 8 of 2010 on Prevention and Eradication of the Crime of Money Laundering (State Gazette of the Republic of Indonesia of 2010 Number 122, Supplement to the State Gazette of the Republic of Indonesia Number 5164). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/232

Manangin, S. A. (2022). The Clause of the Murabahah Financing Agreement in Sharia Banking. *SIGn Jurnal Hukum, 3*(2), 135-150.

https://doi.org/10.37276/sjh.v3i2.160

Manga, A. F. C., & Dianti, F. (2023). Legal Consequences of Unlawful Acts against Banks in Letter of Credit Transactions. *SIGn Jurnal Hukum, 5*(2), 292-311.

https://doi.org/10.37276/sjh.v5i2.292

Oktana, R., Akub, S., & Maskun, M. (2023). Social Media in the Process of Evidence of Electronic Information and Transaction Crimes. *SIGn Jurnal Hukum, 4*(2), 320-

331. https://doi.org/10.37276/sjh.v4i2.252

Orji, U. J. (2019). Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria. *Tilburg Law Review, 24*(1), 105-

124. https://doi.org/10.5334/tilr.137

Paminto, S. R., Amalia, M., Mulyana, A., & Auliya, A. H. (2024). Peran Hukum dalam Melindungi Korban Penipuan Media Sosial Perspektif Sosiologi. *Journal Customary Law, 2*(1), 1-18. https://doi.org/10.47134/jcl.v2i1.3335

Putri, R. A. T., & Sugiyono, H. (2024). Tanggung Jawab Bank terhadap Tindakan Phising dalam Sistem Penggunaan E-Banking (Studi: Kasus Phising pada PT. Bank Rakyat Indonesia (Persero) Tbk). *Jurnal Interpretasi Hukum, 5*(1), 682-690. https://doi.org/10.22225/juinhum.5.1.8318.682-690

Qamar, N., & Rezah, F. S. (2020). *Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal*.

CV. Social Politic Genius (SIGn).a

Regulation of Minister of Trade of the Republic of Indonesia Number 72 of 2020 on the Consumer Dispute Resolution Agency (Bulletin Gazette of the Republic of Indonesia of 2020 Number 1039). https://peraturan.go.id/id/permendag-no-72- tahun-2020

Regulation of the Financial Services Authority of the Republic of Indonesia Number 18/POJK.03/2016 on the Implementation of Risk Management for Commercial Banks (State Gazette of the Republic of Indonesia of 2016 Number 53, Supplement to the State Gazette of the Republic of Indonesia Number 5861). https://peraturan.go.id/id/peraturan-ojk-no-18-pojk-03-2016-tahun-2016

Regulation of the Financial Services Authority of the Republic of Indonesia Number 61/POJK.07/2020 on Alternative Dispute Resolution Agencies in Financial Services Sector (State Gazette of the Republic of Indonesia of 2020 Number 290, Supplement to the State Gazette of the Republic of Indonesia Number 6599). https://peraturan.go.id/id/peraturan-ojk-no-61-pojk-07-2020-tahun-2020

Regulation of the Financial Services Authority of the Republic of Indonesia Number 11/ POJK.03/2022 on the Implementation of Information Technology by Commercial Banks (State Gazette of the Republic of Indonesia of 2022 Number 5/OJK, Supplement to the State Gazette of the Republic of Indonesia Number 5/OJK). https://peraturan.go.id/id/peraturan-ojk-no-11-pojk-03-2022-tahun-2022

Regulation of the Financial Services Authority of the Republic of Indonesia Number 22 of 2023 on Consumer and Public Protection in the Financial Services Sector (State Gazette of the Republic of Indonesia of 2023 Number 40/OJK, Supplement to the State Gazette of the Republic of Indonesia Number 62/OJK). https://peraturan.go.id/id/peraturan-ojk-no-22-tahun-2023

Sampara, S., & Husen, L. O. (2016). *Metode Penelitian Hukum*. Kretakupa Print.

Sari, P., & Sutabri, T. (2023). Analisis Kejahatan Online Phising pada Institusi Pemerintah/Pendidik Sehari-Hari. *Jurnal Digital Teknologi Informasi, 6*(1), 29-34. https://doi.org/10.32502/digital.v6i1.5620

Shapiro, S. J. (2023). *Fancy Bear Goes Phishing: The Dark History of the Information Age, in Five Extraordinary Hacks*. Farrar, Straus and Giroux

Sihombing, R. P., Kusno, K., & Siregar, A. A. (2024). Investigative Effectiveness in the Digital Era: A Case Study of Technological Innovation at the Rokan Hilir Police Resort. *SIGn Jurnal Hukum, 6*(2), 52-67. https://doi.org/10.37276/sjh.v6i2.368

Sinaga, E. P., & Maulisa, N. (2022). The Rights of Creditors of Guarantee Holders in a Limited Liability Company Declared Bankrupt. *SIGn Jurnal Hukum, 4*(1), 72-86. https://doi.org/10.37276/sjh.v4i1.171

Sirait, R. U., Sudirman, L., & Disemadi, H. S. (2025). Legal Protection for Banking Institutions in Small and Medium Enterprise Credit Agreements. *SIGn Jurnal Hukum, 6*(2), 468-481. https://doi.org/10.37276/sjh.v6i2.408

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber. *Sasi, 27*(1), 38-52. https://doi.org/10.47268/sasi.v27i1.394

Suhyana, F. A., Suseno, S., & Ramli, T. S. (2021). Transaksi Ilegal Menggunakan Kartu ATM Milik Orang Lain. *SIGn Jurnal Hukum, 2*(2), 138-156. https://doi.org/10.37276/sjh.v2i2.92

Supriadi, M. R., & Andarsyah, R. (2023). *Deteksi Halaman Website Phishing Menggunakan Algoritma Machine Learning Gradient Boosting Classifier*. Buku Pedia.

Yusuf, D. M. M., Yola, V., Maiharani, D., & Dwi, E. (2022). Analisis terhadap Modus- Modus dalam Hukum Cyber Crime. *Jurnal Hukum, Politik dan Ilmu Sosial, 1*(2), 64-70. https://doi.org/10.55606/jhpis.v1i2.725