JURNAL INOVASI HUKUM
Vol 7, No. 1, Januari 2026
https://ejurnals.com/ojs/index.php/jih

EFEKTIVITAS PERLINDUNGAN HUKUM BAGI NASABAH ATAS KEHILANGAN DANA AKIBAT PHISING DALAM TRANSAKSI DIGITAL BANKING INDONESIA

Bambang Fitrianto[1], Nuri Tania Tarida Aprilia Tampubolon[2], Novi Triana[3], Tia Nazla Ramadhani[4], Deo Hagantha Sembiring[5], Muhammad Fariz Nasution[6]

[1,2,3,4,5,6]Universitas Pembangunan Panca Budi

bambangfitrianto@dosen.pancabudi.ac.id[1], nuritania1306@gmail.com[2], noviicuy@gmail.com[3], tianazla377@gmail.com[4], deohagantha5@gmail.com[5], mfariznst@gmail.com[6]

ABSTRACT; *The improvement of digital technology in the banking field has facilitated the public's ability to conduct financial transactions through electronic banking platforms. However, this progress also raises the threat of cybercrime, such as phishing, which can result in financial losses for customers. This reseacrh tends to assess the legal protection's effectiveness for customers regarding losses due to phishing and banks' liability for such losses, based on the perspective of applicable legal regulations in Indonesia. This study employed a normative juridical technique with a conceptual and statutory approach. The outcomes present that the dispute resolution mechanism through supervision by the Financial Services Authority (OJK) and the Alternative Dispute Resolution Institution for the Financial Services Sector (LAPS SJK) provides a legal basis for protecting financial services users. However, its effectiveness remains limited due to the lack of clear rules on the division of responsibility between banks and customers in phishing cases. Therefore, regulatory strengthening and increased digital education are needed to create stronger and more equitable legal protection for customers in the electronic banking ecosystem.*

Keywords: *Customer Legal Protection, Consequences Of Phishing, Digital Banking Transactions.*

ABSTRAK; Perkembangan teknologi digital dalam sektor perbankan sudah memudahkan masyarakat untuk melakukan transaksi keuangan melalui platform perbankan elektronik. Namun, perkembangan ini juga menimbulkan ancaman kejahatan siber, seperti phishing, yang dapat mengakibatkan kerugian finansial bagi nasabah. Penelitian ini ditujukan guna melaksanakan pengkajia efektivitas perlindungan hukum untuk nasabah terkait kerugian akibat phishing dan tanggung jawab bank atas kerugian tersebut, berdasarkan perspektif aturan perundang-undangan yang diberlakukan di Indonesia. Penelitian ini memakai metode yuridis normatif melalui pendekatan konseptual maupun perundang-undangan. Hasilnya memperlihatkan bahwasanya tata cara penyelesaian sengketa melalui pengawasan Otoritas Jasa Keuangan (OJK) maupun Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK) memberikan landasan hukum untuk melindungi pengguna jasa keuangan. Namun, efektivitasnya masih terbatas karena

belum adanya aturan yang jelas tentang pembagian tanggung jawab antara nasabah dengan bank pada kasus phishing. Oleh karena itu, penguatan regulasi dan peningkatan edukasi digital diperlukan untuk menciptakan perlindungan hukum yang semakin kuat serta berkeadilan untuk nasabah pada ekosistem perbankan elektronik.

Kata Kunci: Perlindungan Hukum Nasabah, Akibat Phishing, Transaksi Perbankan Digital.

PENDAHULUAN

Perkembangan dalam teknologi informasi dan layanan perbankan digital telah memberikan kemudahan yang sangat besar bagi para nasabah. Mereka sekarang bisa melakukan transfer uang dengan cepat, membayar tanpa harus ke teller, dan mengakses rekening mereka lewat aplikasi di ponsel. Namun, kemudahan ini juga membawa risiko baru, terutama kejahatan siber seperti phising yang bertujuan mencuri informasi pribadi dan akses rekening nasabah. Penelitian menunjukkan bahwa kejahatan phising dalam dunia perbankan digital telah menyebabkan kerugian uang yang cukup besar bagi para nasabah.[1]

Di sisi lain, di Indonesia, kerangka perlindungan hukum untuk konsumen telah ditetapkan melalui sejumlah peraturan maupun undang-undang (UU), termasuk UU No. 8 Tahun 1999 terkait Perlindungan Konsumen, UU No. 11 Tahun 2008 terkait Informasi dan Transaksi Elektronik, hingga ketentuan di Bank Indonesia serta Otoritas Jasa Keuangan (OJK) yang mengelola transaksi elektronik. Namun, berbagai penelitian memperlihatkan bahwasanya mekanisme perlindungan hukum untuk nasabah yang terdampak phishing belum optimal, baik dari segi edukasi konsumen, prosedur pelaporan pengaduan, maupun kewajiban bank dalam menangani insiden tersebut.[2]

Dalam konteks ini, penting untuk mengevaluasi sejauh mana hukum mampu melindungi nasabah yang mengalami kerugian finansial akibat phishing dalam aktivitas perbankan elektronik. Efektivitasnya mencakup kapasitas regulasi untuk menegakkan hak-hak nasabah, mekanisme penyelesaian kerugian, dan peran bank dalam mencegah dan menangani insiden

[1] Rismayanti, "Tinjauan Hukum Terhadap Kejahatan Phising dalam Transaksi Elektronik Perbankan," *Jurnal Retentum Fakultas Hukum Universitas Darma Agung*, Vol. 5 No. 2 (2024): 88–97, https://jurnal.darmaagung.ac.id/index.php/retentum/article/download/5380/4464.

[2] Nurul Hidayati, "Perlindungan Hukum Terhadap Nasabah Bank Akibat Kejahatan Siber (Cyber Crime) dalam Transaksi Digital," *Jurnal Cerdika: Jurnal Ilmiah Indonesia*, Vol. 4 No. 3 (2023): 112–123, https://cerdika-temp.publikasiindonesia.id/index.php/cerdika/article/view/2628.

phishing. Beberapa studi memperlihatkan bahwasanya tanggung jawab bank atas kerugian nasabah dikarenakan phishing terbatas terhadap kasus-kasus di mana tidak terdapat kesalahan di pihak mereka, sehingga nasabah seringkali kesulitan dalam mendapatkan kompensasi.[3]

Dengan begitu, penelitian ini ditujukan guna menganalisis efektivitas perlindungan hukum bagi nasabah atas kehilangan dana akibat *phising* dalam transaksi *digital banking* di Indonesia. Dengan demikian diharapkan dapat ditemukan aspek-aspek regulasi yang perlu diperkuat, mekanisme penyelesaian yang lebih jelas, serta rekomendasi praktis bagi bank dan regulator untuk meningkatkan perlindungan bagi nasabah. Penelitian ini penting mengingat semakin masifnya adopsi *digital banking* di Indonesia dan tingginya eksposur nasabah terhadap kejahatan siber.

Permasalahan

Berdasarkan pendahuluan di atas, sejumlah masalah yang ditelaah pada penelitian ini meliputi:

1. Bagaimana mekanisme penyelesaian kerugian nasabah yang berlaku saat ini, dan seberapa efektif mekanisme tersebut dalam menyelesaikan kasus kehilangan dana akibat phishing pada transaksi perbankan digital di Indonesia?
2. Bagaimana tanggung jawab bank atas kerugian nasabah dikarenakan phishing dalam layanan perbankan digital, baik dari segi hukum maupun penerapannya dalam praktik perbankan?

METODE PENELITIAN

Penelitian ini dilakukan memakai metode yuridis normatif, yakni teknik penelitian hukum yang berpusat kepada peraturan perundang-undangan (law in books) dan implementasinya pada praktik hukum (law in action).[4] Metode ini dipilih karena penelitian ini ditujukan guna melaksanakan pengkajian aturan perundang-undangan yang ada di Indonesia yang melindungi nasabah dari kerugian akibat phishing dalam transaksi perbankan digital. Penelitian ini memakai pendekatan konseptual serta perundang-undangan.[5] Pendekatan hukum ditujukan guna menelaah berbagai aturan perundang-undangan yang mengarahkan terkait

[3] Komang Dwi Cahyani dan I Gusti Bagus Dwi Kresna, "Tanggung Jawab Bank terhadap Kerugian Nasabah Akibat Kejahatan Phising," *Kertha Semaya: Journal Ilmu Hukum*, Universitas Udayana, Vol. 12 No. 4 (2024): 1567– 1580, https://ojs.unud.ac.id/index.php/kerthasemaya/article/view/114466.

[4] Soerjono Soekanto dan Sri Mamudji, Penelitian Hukum Normatif: Suatu Tinjauan Singkat, Jakarta: RajaGrafindo Persada, 2019.

[5] Peter Mahmud Marzuki, Penelitian Hukum, Edisi Revisi, Jakarta: Kencana, 2021.

perlindungan konsumen dalam bidang layanan keuangan. Peraturan perundang-undangan tersebut mencakup UU No. 19 Tahun 2016 terkait Informasi dan Transaksi Elektronik, UU No. 8 Tahun 1999 terkait Perlindungan Konsumen, hingga Peraturan OJK yang dikenal sebagai POJK No. 1/POJK.07/2013 terkait Perlindungan Konsumen di Sektor Jasa Keuangan.[6] Sedangkan pendekatan konseptual dipergunakan dalam menelaah pengertian hukum tentang akuntabilitas bank maupun perlindungan hukum untuk nasabah perbankan digital.[7]

Data sekunder yang didapat dari penelitian kepustakaan merupakan jenis data yang dipergunakan dalam studi ini.[8] Data sekunder tersebut di antaranya:

1. Bahan hukum primer, di antaranya peraturan perundang-undangan yang mengatur transaksi elektronik dan perlindungan konsumen jasa keuangan;
2. Bahan hukum sekunder, mencakup jurnal ilmiah, buku, hasil studi sebelumnya yang relevan, serta artikel hukum; dan
3. Bahan hukum tersier, yakni ensiklopedia maupun kamus hukum, yang dipergunakan dalam menerangkan lebih jelas konsep hukum yang dipakai pada analisis.[9]

Metode analisis data yang dipergunakan yakni kualitatif dengan menguraikan data secara analitis dan deskriptif. Tujuan analisis ini adalah untuk mengungkap efektivitas peraturan perundang-undangan yang relevan dalam praktik, khususnya mengenai perlindungan hukum bagi konsumen korban phishing.[10] Tujuan analisis ini yakni guna memberi penggambaran komprehensif terkait bagaimana teori perlindungan hukum berkaitan dengan fakta di industri perbankan digital Indonesia.

HASIL DAN PEMBAHASAN

A. Mekanisme Penyelesaian Kerugian Nasabah dan Efektivitasnya dalam Praktik

Beberapa undang-undang penting di Indonesia telah mengatur bagaimana menangani kerugian nasabah yang terjadi karena phishing melalui transaksi digital banking. POJK No. 1/POJK.07/2013 terkait Perlindungan Konsumen Sektor Jasa Keuangan menetapkan bahwasanya perusahaan layanan keuangan harus mempunyai sistem penanganan pengaduan

[6] Otoritas Jasa Keuangan, Peraturan OJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, https://peraturan.bpk.go.id/Home/Details/25922/pojk-no-1pojk072013
[7] Achmad Ali, Menguak Teori Hukum dan Teori Peradilan (Vol. I), Jakarta: Kencana, 2018.
[8] Amiruddin dan Zainal Asikin, Pengantar Metode Penelitian Hukum, Jakarta: Raja Grafindo Persada, 2018.
[9] Bambang Waluyo, Penelitian Hukum Dalam Praktek, Jakarta: Sinar Grafika, 2019.
[10] OJK, Laporan Perlindungan Konsumen Sektor Jasa Keuangan 2024, diakses 1 November 2025, https://www.ojk.go.id

konsumen yang cepat, jelas, dan bertanggung jawab.[11] Di sisi lain, Surat Edaran OJK No. 17/SEOJK.07/2014 menetapkan standar teknis penyelenggaraan pengaduan, yang mencakup batas waktu bank untuk menanggapi dan menyelesaikan pengaduan.[12]

Secara umum, penyelesaian kerugian nasabah akibat phishing dapat dilakukan melalui tiga tahapan mekanisme, yaitu:

1. Penyelesaian Internal di Bank

   Jika seorang nasabah mengalami kerugian, mereka bisa melapor ke bank di mana mereka memiliki rekening. Bank harus melakukan pemeriksaan dan penyelidikan awal untuk memastikan apakah laporan itu benar.[13] Sesuai dengan aturan OJK, bank perlu memberikan jawaban awal dalam waktu maksimum 20 hari kerja setelah laporan diterima.[14] Pada tahap ini, biasanya solusi yang diberikan berupa pengembalian uang, kompensasi, atau bisa juga penolakan dengan alasan tertentu, seperti jika ada dugaan kesalahan dari nasabah.

2. Penyelesaian dengan Lembaga Alternatif Penyelesaian Sengketa (LAPS SJK)

   Bila nasabah merasakan ketidakpuasan atas penanganan dari suatu lembaga, nasabah bisa menyampaikan keluhannya pada LAPS SJK.[15] LAPS SJK bertindak sebagai pihak netral dan membantu mediasi antara nasabah dan lembaga keuangan tanpa harus melalui pengadilan. Proses ini non-hukum, cepat, dan murah. Bahkan, sebagian besar permasalahan perbankan digital yang diajukan ke LAPS SJK diselesaikan dalam waktu kurang dari 60 hari kerja.[16]

3. Penyelesaian Melalui Jalur Litigasi (Pengadilan)

   Nasabah berhak melakukan pengajuan gugatan ke pengadilan jika sistem penangan di luar pengadilan tidak menghasilkan kepuasan. Para konsumen dapat menuntut penyedia jasa yang menyebabkan kerugian, baik secara individu maupun melalui badan perlindungan konsumen, berlandaskan ketetapan Pasal 45 UU No. 8 Tahun 1999 terkait

[11] OJK, Peraturan OJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen di Sektor Jasa Keuangan, https://peraturan.bpk.go.id/Home/Details/25922/pojk-no-1pojk072013
[12] OJK, Surat Edaran OJK No. 17/SEOJK.07/2014 tentang Pedoman Pelaksanaan Layanan Pengaduan Konsumen, https://www.ojk.go.id
[13] Bank Indonesia, Blueprint Sistem Pembayaran Indonesia 2025, Jakarta: Bank Indonesia, 2020.
[14] OJK, Pedoman Penanganan Pengaduan Konsumen Sektor Jasa Keuangan, 2023, https://www.ojk.go.id
[15] LAPS SJK, Pedoman Penyelesaian Sengketa Konsumen Sektor Jasa Keuangan, 2023, https://lapssjk.id
[16] Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK), Pedoman Penyelesaian Sengketa Konsumen Sektor Jasa Keuangan, 2023, https://lapssjk.id

Perlindungan Konsumen (UUPK).[17] Meskipun demikian, sejumlah besar korban penipuan phishing menghindari jalur hukum karena prosedurnya dianggap rumit dan memakan waktu.

Meskipun aturan telah menawarkan banyak solusi, implementasinya masih belum optimal. Pertama dan terpenting, banyak nasabah yang belum memahami hak mereka untuk mengajukan pengaduan. Sebagai hasil dari survei OJK yang dilakukan pada tahun 2024, hanya sekitar 41% konsumen jasa keuangan yang mengetahui adanya mekanisme pengaduan resmi di bawah LAPS SJK atau OJK.[18]

Kedua, bank sering menolak bertanggung jawab atas kerugian klien dengan alasan phishing terjadi di luar sistem keamanan mereka.[19] Padahal, teori perlindungan hukum Philipus M. Hadjon memaparkan bahwasanya perlindungan hukum harus diberikan baik sebelum (preventif) maupun sesudah (represif) pelanggaran hak konsumen.[20] Dalam situasi seperti ini, bank seharusnya tidak hanya bertanggung jawab untuk menjaga sistem, tetapi juga harus memberi tahu pelanggan tentang mitigasi risiko dan edukasi.

Ketiga, hambatan besar lainnya adalah keterbatasan teknologi pelacakan kejahatan siber. Sebagian besar pelaku phishing beroperasi dari berbagai negara dan menggunakan jaringan virtual private network (VPN) dan rekening penampung, yang membuatnya sulit untuk dilacak.[21] Hal ini membuat pengembalian dana hampir tidak mungkin, bahkan setelah laporan dibuat ke bank dan polisi.

Keempat, lembaga penegak hukum dan otoritas keuangan belum bekerja sama dengan baik. Banyak kasus kehilangan uang karena phishing hanya dilaporkan dan tidak ada tindakan hukum yang jelas.[22]

Oleh karena itu, kerangka hukum yang dirancang untuk melindungi pelanggan masih kurang efektif karena kekurangan pengawasan, edukasi publik, dan penegakan hukum siber. Perlindungan hukum ideal harus mampu memberikan kepastian hukum

[17]Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen, https://peraturan.bpk.go.id/Home/Details/45002/uu-no-8-tahun-1999
[18] OJK, Laporan Perlindungan Konsumen Sektor Jasa Keuangan 2024, diakses 1 November 2025, https://www.ojk.go.id
[19] Dwi Wulandari, "Efektivitas Perlindungan Hukum Nasabah Bank Dalam Transaksi Digital," Jurnal Hukum dan Pembangunan Ekonomi, 2023, https://ejournal.unair.ac.id/JHPE/article/view/4567
[20] Philipus M. Hadjon, Perlindungan Hukum Bagi Rakyat Indonesia, Surabaya: Bina Ilmu, 1987.
[21] Kementerian Kominfo, Laporan Keamanan Siber Indonesia 2024, Jakarta: Kominfo, 2024.
[22] CNN Indonesia, "Bareskrim Sebut Banyak Kasus Phishing Mandek di Pelaporan," CNNIndonesia.com, 2024, https://www.cnnindonesia.com/teknologi/phishing-bareskrim

serta keamanan untuk konsumen serta menyeimbangkan tanggung jawab antara bank dan pengguna layanan digital.

B. Tanggung Jawab Bank terhadap Kerugian Nasabah Akibat Phishing

Masalah tanggung jawab bank atas kerugian nasabah yang terjadi melalui penipuan phishing dalam layanan perbankan online cukup rumit, karena mencakup aspek hukum, inovasi teknologi, serta kepercayaan masyarakat terhadap institusi perbankan. Prinsip kewaspadaan atau prinsip kehati-hatian merupakan landasan hukum utama di Indonesia yang mengatur pertanggungjawaban ini. Lebih lanjut, bank wajib menjamin keamanan sistem digital yang digunakan dalam setiap transaksi.[23] Dari segi hukum, setiap operator sistem elektronik harus mengoperasikan platform yang handal, terlindungi, dan akuntabel, sebagaimana tercantum di Pasal 15 ayat (3) UU No. 11 Tahun 2008 yang berubah menjadi UU No. 19 Tahun 2016.[24] Bank bisa dikenai tanggung jawab hukum jika ada kekurangan dalam mekanisme keamanan digital mereka yang mengakibatkan rugi bagi klien. Selain itu, aturan umum mengenai tindakan yang melanggar hukum ditetapkan melalui Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata), yang menekankan bahwasanya tiap tindakan yang merugikan pihak lain akibat kesalahan atau kelalaian harus diganti oleh pelaku yang bertanggung jawab.[25] Dengan demikian, bank dapat dianggap bertanggung jawab jika terbukti ceroboh dalam menjaga informasi atau aktivitas nasabah dari ancaman phishing.

Karena sebagian besar kasus phishing disebabkan oleh kelalaian nasabah sendiri, seperti memberikan One Time Password (OTP), kata sandi, atau tautan pribadi kepada pelaku, tanggung jawab bank sering kali menjadi perdebatan. Bank biasanya berpendapat bahwa pada kasus yang demikian, nasabah mempunyai tanggung jawab atas kerugian karena tindakan tersebut melanggar syarat dan ketentuan penggunaan layanan digital banking yang telah disepakati saat pembukaan rekening.[26] Sebagian besar bank di Indonesia menggunakan kebijakan zero liability terbatas, yang berarti bahwa bank tidak akan menanggung kerugian jika terbukti bahwa pelanggan melakukan kelalaian pribadi. Namun, bank bertanggung jawab

[23] OJK, POJK No. 12/POJK.03/2021 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum, https://peraturan.bpk.go.id/Home/Details/214061/pojk-no-12pojk032021

[24] Undang-Undang No. 11 Tahun 2008 jo. Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, https://peraturan.bpk.go.id/Home/Details/37575/uu-no-19-tahun-2016

[25] Kitab Undang-Undang Hukum Perdata, Pasal 1365, https://peraturan.bpk.go.id/Home/Details/49401/kuhperdata

[26] Bank Indonesia, Peraturan Bank Indonesia No. 22/23/PBI/2020 tentang Sistem Pembayaran, https://peraturan.bpk.go.id/Home/Details/169446/pbi-no-2223pbi2020

untuk mengganti uang sepenuhnya kepada klien jika kerugian terjadi karena kebocoran data internal atau masalah sistem keamanan bank. Tidak ada standar yang jelas di sistem hukum Indonesia tentang bagaimana membagi tanggung jawab dalam kasus kejahatan siber, seperti yang ditunjukkan oleh perdebatan tentang batas tanggung jawab bank dan nasabah ini. Prinsip tanggung jawab berbagi digunakan di sejumlah negara, selayaknya Australia serta Inggris, yang mana bank dan konsumen ditanggung sesuai tingkat kesalahan masing-masing pihak. Konsep ini bisa menjadi rujukan bagi Indonesia dalam memperkuat kerangka hukum perbankan digital di masa depan.

Teori tanggung jawab hukum juga dikenal sebagai teori pertanggungjawaban hukum menekankan bahwa pihak yang memiliki kendali terhadap risiko harus menanggung konsekuensi hukum yang timbul dari risiko tersebut.[27] Bank memiliki kewajiban hukum sebagai penyedia sistem dan pengelola data nasabah untuk menjaga keamanan data, melakukan audit sistem secara teratur, dan menetapkan mekanisme kompensasi yang jelas untuk kerugian yang disebabkan oleh kegagalan sistem. Bank memiliki tugas normatif dan moral. Mereka juga harus menjaga kepercayaan masyarakat terhadap sistem perbankan digital. Kegagalan bank untuk menangani kasus phishing secara terbuka dapat menurunkan kepercayaan publik dan menghalangi transformasi digital sektor keuangan nasional. Oleh karena itu, sebagai langkah pencegahan, sejumlah bank besar di Indonesia kini mulai menerapkan program literasi digital, pemberitahuan keamanan langsung, dan peningkatan sistem autentikasi multifaktor.[28]

Dari uraian tersebut, dapat disimpulkan bahwasanya tanggung jawab bank atas kerugian nasabah dikarenakan phishing bersifat dua lapis, yaitu:

1. Tanggung jawab preventif, berupa kewajiban menjamin keamanan sistem elektronik, memberikan edukasi kepada nasabah, serta menerapkan teknologi perlindungan siber yang memadai; dan
2. Tanggung jawab represif, yaitu mengganti kerugian nasabah apabila terbukti adanya kelalaian atau kegagalan sistem yang menyebabkan bocornya data dan hilangnya dana nasabah.[29]

[27] Hans Kelsen, General Theory of Law and State, Cambridge: Harvard University Press, 1945.
[28] Bank Mandiri, Laporan Keberlanjutan 2023: Perlindungan Data dan Literasi Digital Nasabah, https://bankmandiri.co.id
[29] Tri Handayani, "Penerapan Prinsip Strict Liability Dalam Perlindungan Nasabah Digital Banking," Jurnal Ilmu Hukum Aktualita, 2023, https://ejournal.unri.ac.id/index.php/aktualita

Namun, pembaruan regulasi diperlukan untuk memastikan standar minimal keamanan sistem perbankan digital dan mekanisme kompensasi yang adil bagi korban phishing agar perlindungan hukum menjadi efektif. Dalam hal ini, ahli seperti Bamabang Fitrianto mengatakan bahwa industri perbankan harus meningkatkan penerapan standar kehati-hatian dan perlindungan konsumen dalam seluruh layanan digital untuk menghentikan peningkatan risiko siber.[30]

KESIMPULAN

Pertama, cara untuk menyelesaikan masalah kerugian yang dialami nasabah lewat lembaga seperti LAPS SJK dan pengaduan ke OJK sudah memberi kesempatan resmi bagi korban untuk mendapatkan hak mereka. Namun, cara ini belum sepenuhnya berhasil karena sering kali prosesnya lama dan hasilnya tidak selalu mengikat bank.

Kedua, ada kekurangan dalam peraturan yang memaparkan pertanggungjawaban bank atas kerugian nasabah yang disebabkan oleh phishing. Meskipun seharusnya bank wajib menjaga keamanan sistem elektroniknya, dalam prakteknya banyak kasus di mana nasabah justru harus menanggung kerugian karena dianggap lalai.

Dengan begitu, perlindungan hukum untuk nasabah masih kurang efektif dan lebih reaktif, belum meliputi pencegahan serta kompensasi dengan baik. Diperlukan peningkatan kebijakan, edukasi digital untuk masyarakat, dan penerapan tanggung jawab hukum yang seimbang antara bank dan nasabah agar keadilan dan kepastian hukum bisa tercapai di era perbankan digital.

Saran

1. Bagi Pemerintah dan Regulator (OJK dan BI):

   Perlu dijelaskan lebih lanjut mengenai aturan tentang siapa yang bertanggung jawab antara bank dan nasabah ketika terjadi kejahatan daring seperti phishing. Ini juga termasuk penerapan prinsip tanggung jawab bersama yang sudah diterapkan di beberapa negara maju.
2. Bagi Pihak Bank

   Diharapkan audit berkala, penerapan authentication multi-factor, dan pengawasan internal terhadap potensi kebocoran data akan meningkatkan sistem keamanan teknologi

[30] Bambang Fitrianto, Hukum Jasa Keuangan dan Perlindungan Konsumen (Jakarta:Sinar Grafika,2021),87

informasi. Selain itu, bank harus membentuk tim respons cepat (cyber fraud response team) untuk secara transparan dan cepat menangani laporan kehilangan dana.

3. Bagi Nasabah

   Meningkatkan kewaspadaan dalam menjaga kerahasiaan data pribadi, menghindari berbagi OTP dan tautan dengan pihak yang tidak resmi, dan segera melaporkan potensi penipuan digital kepada bank dan OJK.

4. Bagi Akademisi dan Peneliti Hukum

   Perlu dilanjutkan penelitian tentang cara melindungi hukum yang bias disesuaikan dalam transaksi perbankan digital. Penelitian ini harus memasukkan bagian tentang teknologi,hukum,dan kebiasaan konsumen yang menggunakan digital

DAFTAR PUSTAKA

Achmad Ali. (2018). *Menguak Teori Hukum dan Teori Peradilan* (Vol. I). Jakarta: Kencana.

Amiruddin, & Asikin, Z. (2018). *Pengantar Metode Penelitian Hukum*. Jakarta: RajaGrafindo Persada.

Australian Competition and Consumer Commission (ACCC). (2023). *Targeting Scams Report 2023*. Canberra: ACCC. https://www.accc.gov.au

Bank Indonesia. (2020). *Blueprint Sistem Pembayaran Indonesia 2025*. Jakarta: Bank Indonesia.

Bank Indonesia. (2020). *Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran*. https://peraturan.bpk.go.id/Home/Details/169446/pbi-no-2223pbi2020

Bank Mandiri. (2023). *Laporan Keberlanjutan 2023: Perlindungan Data dan Literasi Digital Nasabah*. https://bankmandiri.co.id

Bambang Fitrianto. (2021). *Hukum Jasa Keuangan dan Perlindungan Konsumen*. Jakarta: Sinar Grafika.

Bambang Waluyo. (2019). *Penelitian Hukum Dalam Praktek*. Jakarta: Sinar Grafika.

CNN Indonesia. (2024). "Bareskrim Sebut Banyak Kasus Phishing Mandek di Pelaporan." https://www.cnnindonesia.com/teknologi/phishing-bareskrim

Cahyani, K. D., & Kresna, I. G. B. D. (2024). "Tanggung Jawab Bank terhadap Kerugian Nasabah Akibat Kejahatan Phising." *Kertha Semaya: Journal Ilmu Hukum*, 12(4), 1567–1580. https://ojs.unud.ac.id/index.php/kerthasemaya/article/view/114466

Dwi Wulandari. (2023). "Efektivitas Perlindungan Hukum Nasabah Bank Dalam Transaksi Digital." *Jurnal Hukum dan Pembangunan Ekonomi*. https://ejournal.unair.ac.id/JHPE/article/view/4567

Hadjon, P. M. (1987). *Perlindungan Hukum Bagi Rakyat Indonesia*. Surabaya: Bina Ilmu.

Hans Kelsen. (1945). *General Theory of Law and State*. Cambridge: Harvard University Press.

Hidayati, N. (2023). "Perlindungan Hukum Terhadap Nasabah Bank Akibat Kejahatan Siber (Cyber Crime) dalam Transaksi Digital." *Jurnal Cerdika: Jurnal Ilmiah Indonesia*, 4(3), 112–123. https://cerdika-temp.publikasiindonesia.id/index.php/cerdika/article/view/2628

Kementerian Kominfo. (2024). *Laporan Keamanan Siber Indonesia 2024*. Jakarta: Kominfo.

Kitab Undang-Undang Hukum Perdata. Pasal 1365. https://peraturan.bpk.go.id/Home/Details/49401/kuhperdata

LAPS SJK. (2023). *Pedoman Penyelesaian Sengketa Konsumen Sektor Jasa Keuangan*. https://lapssjk.id

Marzuki, P. M. (2021). *Penelitian Hukum* (Edisi Revisi). Jakarta: Kencana.

Nurul Hidayati. (2023). "Perlindungan Hukum Terhadap Nasabah Bank Akibat Kejahatan Siber (Cyber Crime) dalam Transaksi Digital." *Jurnal Cerdika*, 4(3), 112–123.

OJK. (2023). *Pedoman Penanganan Pengaduan Konsumen Sektor Jasa Keuangan*. https://www.ojk.go.id

OJK. (2024). *Laporan Perlindungan Konsumen Sektor Jasa Keuangan 2024*. Diakses 1 November 2025. https://www.ojk.go.id

Otoritas Jasa Keuangan. (2013). *Peraturan OJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan*. https://peraturan.bpk.go.id/Home/Details/25922/pojk-no-1pojk072013

Otoritas Jasa Keuangan. (2014). *Surat Edaran OJK Nomor 17/SEOJK.07/2014 tentang Pedoman Pelaksanaan Layanan Pengaduan Konsumen*. https://www.ojk.go.id

Otoritas Jasa Keuangan. (2021). *POJK Nomor 12/POJK.03/2021 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum*. https://peraturan.bpk.go.id/Home/Details/214061/pojk-no-12pojk032021

Putri, R. A. T. (2024). "Tanggung Jawab Bank Terhadap Tindakan Phishing Dalam Layanan Digital."*JuinHum*. https://ejournal.warmadewa.ac.id/index.php/juinhum/article/download/8318/5179

Rismayanti. (2024). "Tinjauan Hukum Terhadap Kejahatan Phising dalam Transaksi Elektronik Perbankan." *Jurnal Retentum Fakultas Hukum Universitas Darma Agung*, 5(2), 88–97. https://jurnal.darmaagung.ac.id/index.php/retentum/article/download/5380/4464

Soerjono Soekanto & Mamudji, S. (2019). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: RajaGrafindo Persada.

Tri Handayani. (2023). "Penerapan Prinsip Strict Liability Dalam Perlindungan Nasabah Digital Banking." *Jurnal Ilmu Hukum Aktualita*. https://ejournal.unri.ac.id/index.php/aktualita

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. https://peraturan.bpk.go.id/Home/Details/45005/uu-no-8-tahun-1999

Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. https://peraturan.bpk.go.id/Home/Details/37575/uu-no-19-tahun-2016