# PERLINDUNGAN HUKUM TERHADAP KEAMANAN DANA NASABAH BANK DALAM KASUS PHISHING [1]

**Oleh :**
**Azarya E. Mamesah [2]**
**Grace H. Tampongangoy[3]**
**Sarah D. L. Roeroe[4]**

## ABSTRAK

Penelitian ini bertujuan untuk mengetahui pengaturan perlindungan hukum dalam melindungi dana nasabah bank dari serangan phisihing dan untuk mengetahui pelaksanaan perlindungan hukum bank terhadap nasabah korban phishing. Dengan menggunakan metode penelitian yuridis normatif, dapat ditarik kesimpulan yaitu : 1. Perlindungan hukum terhadap dana nasabah bank dari serangan phishing diatur secara cukup komprehensif melalui berbagai peraturan perundang-undangan, seperti UndangUndang Perlindungan Konsumen, Undang-Undang Informasi dan Transaksi Elektronik, serta regulasi dari Otoritas Jasa Keuangan (OJK). 2. Pelaksanaan perlindungan hukum bank terhadap nasabah korban phishing di Indonesia yaitu regulasi yang masih bersifat umum dan kurang spesifik terhadap kasus phishing, seperti yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta regulasi Otoritas Jasa Keuangan (OJK), yang sering kali tidak menjangkau aspek tanggung jawab bank secara detail. Selain itu, keterbatasan teknologi keamanan di sistem perbankan, kurangnya koordinasi antara bank dengan aparat penegak hukum, serta rendahnya literasi digital nasabah menjadi faktor penghambat utama dalam penanganan kasus.

Kata Kunci : *keamanan, nasabah bank, phising*

## PENDAHULUAN

### A. Latar Belakang

Salah satu kelemahan signifikan dari e-banking adalah potensi terjadinya kejahatan perbankan seperti phising, di mana pelaku dari luar bank berpura-pura menjadi pihak yang dapat dipercaya dan berusaha mendapatkan Informasi pribadi seperti nama lengkap, nomor telepon, alamat email, dan detail kartu kredit klien, kemudian memaksa korban untuk mengklik tautan pemancing. Pasal 30 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyatakan bahwa tindakan ilegal ini adalah pelanggaran terhadap pasal tersebut. Hal ini dinyatakan karena pelaku phishing berusaha untuk menembus sistem keamanan bank agar dapat menarik seluruh dana yang tersimpan di rekening korban, dengan tujuan untuk membobol akun nasabah yang menjadi target mereka.[3] Peraturan Otoritas Jasa Keuangan Nomor 6/POJK.07/2022 Tahun 2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan memberikan panduan terkait tanggung jawab bank terhadap potensi kerugian yang dialami nasabah akibat kejahatan siber tersebut. Peraturan ini bertujuan untuk memastikan bahwa bank tidak hanya bertanggung jawab dalam menanggulangi risiko kejahatan siber, tetapi juga dalam memberikan perlindungan dan pemulihan kepada nasabah yang menjadi korban.[5]

Peranan bank dalam mengatasi kerugian yang dialami nasabah akibat phising semakin krusial karena berhubungan dengan kepercayaan masyarakat terhadap lembaga perbankan. Institusi keuangan diharapkan memiliki pedoman yang tegas dan terbuka terkait proses penanganan keluhan serta pengembalian dana bagi nasabah yang terkena dampak. Nasabah merupakan pelanggan bank yang berhak mendapatkan informasi tentang dana mereka melalui layanan yang disediakan. Oleh karena itu, perlindungan terhadap konsumen konsumen merupakan suatu hal yang wajib diperhatikan dengan serius dan tidak dapat diabaikan.[6] Hak nasabah yang menyimpan fokus pada usaha untuk menagih dan mendapatkan kembali uang yang telah mereka simpan. Kelalaian dari pihak bank harus ditindaklanjuti melalui pengawasan, mengingat bahwa bank memiliki tugas untuk memberikan layanan kepada masyarakat dalam menyimpan uang dengan cara yang aman. Selain itu, kerjasama antara bank, pemerintah, dan organisasi terkait sangat penting untuk membangun sistem perbankan yang andal, dan aman.[6]

Sesuai dengan Peraturan OJK Nomor 6/POJK.07/2022 Tahun 2022 tentang Perlindungan Konsumen di Sektor Keuangan, bank bertanggung jawab untuk menjaga kerahasiaan data dan dana pelanggan. Dalam kasus kehilangan akibat phishing, tanggung jawab bank menjadi sangat krusial, terutama jika

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 210711011006
[3] Fakultas Hukum Unsrat, Magister Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] Peraturan Otoritas Jasa Keuangan Nomor 6/POJK.07/2022 Tahun 2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan
[6] Siti Fatimah, 'Tinjauan Yuridis Terhadap Pelaku Tindak Pidana Perjudian Online Di Indonesia', Innovative: Journal Of Social Science Research, 3.2 (2023), pp. 3224–31.

terdapat bukti kelalaian dalam prosedur keamanan yang diterapkan. Penelitian ini mengungkapkan bahwa banyak pelanggan yang terjebak dalam phishing disebabkan oleh kurangnya pengetahuan mereka tentang praktik keamanan digital serta minimnya informasi yang diberikan oleh bank. Dalam aspek hukum, bank diwajibkan untuk menerapkan manajemen risiko yang baik, termasuk dalam hal perlindungan nasabah. Hal ini ditegaskan dalam aturan yang mewajibkan bank memiliki sistem keamanan yang memadai. Namun, sering kali nasabah tidak tahu bagaimana cara mengajukan klaim atau langkah apa yang harus dilakukan setelah mereka menjadi korban. Proses klaim pun acapkali dipenuhi dengan birokrasi yang membuat nasabah kebingungan..

Contoh kasus Phishing yang pernah terjaadi di Indonesia adalah kasus yang melibatkan Silvia Yap, seorang nasabah prioritas di BRI KCP Lawang, Malang, Jawa Timur, yang menjadi target serangan phishing pada Mei 2023. Dalam kejadian ini, jumlah saldo di rekening Silvia Yap menurun drastis sebanyak Rp 1.446.000.000 dalam waktu singkat. Melalui aplikasi WhatsApp, korban mendapatkan pesan yang berisi undangan dalam bentuk apk, yang menjadi awal dari kasus ini. Setelah korban mengklik dan membuka undangan itu, berbagai iklan mulai muncul di perangkatnya. Penurunan saldo tabungan dan transfer dana melalui fitur pengiriman antar rekening di e-banking menjadi masalah serius ketika korban menyadari bahwa saldonya hampir habis, hanya tersisa Rp 2 juta. Keesokan harinya, korban menghubungi Bank BRI KCP Lawang untuk menanyakan mengenai masalah keamanan dan meminta agar dananya dikembalikan. Namun sayangnya permintaan tersebut tidak dapat dipenuhi oleh BRI KCP Lawang. Mereka menyatakan bahwa bank hanya akan mengganti kerugian nasabah jika disebabkan oleh kesalahan yang terjadi dalam layanan perbankan. Situasi ini menampilkan bahwa bank beranggapan bahwa kejadian tersebut bukan akibat kesalahan dalam layanan perbankan yang mereka tawarkan, sehingga tanggung jawab atas kerugian tersebut tidak dapat dipikul oleh pihak bank.[7]

Dalam situasi kehilangan uang karena phishing, tanggung jawab bank dapat diukur berdasarkan sejauh mana mereka telah memenuhi kewajiban tersebut. Bank diwajibkan untuk menunjukkan bahwa mereka telah mengambil semua langkah pencegahan yang diperlukan, seperti memberikan edukasi tentang keamanan dalam transaksi digital kepada nasabah. Hal ini dapat dilakukan dengan berbagai cara, seperti melaksanakan kampanye edukasi yang bertujuan meningkatkan kesadaran konsumen akan pentingnya kewaspadaan saat bertransaksi, serta memberikan saran dan panduan terkait keamanan transaksi digital, termasuk hal-hal yang sebaiknya

**B. Rumusan Masalah**

1. Bagaimana pengaturan perlindungan hukum dalam melindungi dana nasabah bank dari serangan phishing?
2. Bagaimana pelaksanaan perlindungan hukum bank terhadap nasabah korban phising?

**C. Metode Penelitian**

Metode pendekatan yang digunakan dalam penelitian ini adalah metode pendekatan yuridis normatif.

**PEMBAHASAN**

**A. Pengaturan Perlindungan Hukum Dalam Melindungi Dana Nasabah Bank Dari Serangan Phishing**

Perbankan dalam menjalankan usaha atau kegiatannya adalah adanya tingkat kepercayaan masyarakat terhadap bank. Semakin tinggi minat masyarakat untuk menyimpan atau menanamkan dana di bank, maka semakin tinggi pula tingkat kepercayaan masyarakat terhadap bank tersebut. Jika jumlah dana yang disimpan atau ditarik oleh masyarakat dari bank tergolong besar, hal ini menunjukkan bahwa tingkat kepercayaan masyarakat terhadap bank sangat rendah. Oleh karena itu, sangat wajar untuk menata, membangun, dan meningkatkan tingkat kepercayaan masyarakat terhadap bank melalui berbagai peraturan perundang-undangan yang dapat memberikan kepastian tentang hak, kewajiban, serta keselamatan dana yang disimpan oleh nasabah. Selain itu, hal yang tidak kalah penting adalah bahwa lembaga perbankan memiliki peluang dan kesempatan untuk mencapai visi dan misi strategis dalam pembangunan bangsa dan negara. Membangun bangsa dan negara memang sangat penting, terutama dalam menjaga stabilitas perekonomian yang pada akhirnya akan mempengaruhi kesejahteraan masyarakat. [8]

Kejahatan bisa terjadi di mana saja, termasuk jenis baru yaitu cyber crime atau kejahatan siber. Kejahatan siber adalah bentuk kejahatan modern yang baru saja muncul dan telah menarik perhatian internasional. Volodymyr Golubev menyebutnya sebagai perilaku antisosial yang

[7] Ali, A. Nasabah Prioritas Bank BRI Kehilangan Rp 1,4 Miliar Akibat Phising, Sambangi Polda Jatim. Berita Sat.(2023).

[8] Moho, H., Ndruru, A., & Laowo, Y. (2023). Analisis Hukum Terhadap Perlindungan Dana Nasabah Pada Bank. Jurnal Panah Keadilan, 2(2), 8-15.

baru. Kejahatan ini tidak bisa diabaikan karena sekarang hampir semua sektor menggunakan sistem digital yang menjadi tempat berlangsungnya kejahatan tersebut. Untuk mencegah kejahatan ini, banyak langkah yang perlu dilakukan dan masyarakat harus sadar. Namun, pemerintah juga harus terlibat dalam menjaga keamanan dan menjadi perlindungan utama bagi masyarakat dari kejahatan tersebut.[9]

Phishing adalah serangan siber di mana orang jahat berpura-pura sebagai lembaga atau orang yang dianggap aman, agar bisa mengambil informasi penting dari korban, seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya. Cara yang digunakan biasanya melalui email, pesan SMS, atau situs web palsu yang tampak seperti hal yang sah. Serangan ini bisa menyebabkan kerugian uang, pencurian identitas, atau kebocoran data. Karena itu, penting bagi kita untuk selalu meningkatkan kesadaran dan mengetahui cara mengenali serta menghindari serangan phishing agar tetap aman dari ancaman tersebut.

Phishing adalah upaya memperoleh informasi pribadi seseorang dengan menggunakan teknik penipuan. Data yang biasanya di-phishing mencakup informasi pribadi (nama, umur, alamat), informasi akun (nama pengguna dan kata sandi), dan informasi keuangan (informasi kartu kredit, akun). Istilah resmi untuk phishing adalah phishing, dan asal usulnya adalah ``fishing'' yang berarti “memancing." Phishing bertujuan untuk mengelabui orang agar mengungkapkan informasi pribadi tanpa sepengetahuan mereka. Informasi yang diberikan akan digunakan untuk tujuan kriminal[10]

Phishing diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Meski begitu, aturan mengenai phishing masih terasa kurang jelas dan terdapat kekaburan dalam hukumnya. Secara umum, phishing adalah tindakan membuat situs web palsu yang tampil mirip dengan situs resmi. Pelaku kemudian mengirimkan email, pesan, atau tautan ke korban agar mereka mengakses situs tersebut. Tujuannya adalah agar korban memasukkan informasi pribadi yang sensitif, seperti username, password, nomor kartu kredit, dan lainnya. Setelah itu, informasi tersebut digunakan oleh pelaku secara ilegal, sehingga merugikan korban. Pasal 35 dan 28 di dalam UU ITE belum sepenuhnya mencakup unsur phishing sebagai tindakan yang melibatkan manipulasi data dan penipuan secara utuh. Oleh karena itu, disarankan untuk menyusun konsep phishing yang lebih jelas serta merevisi Pasal 35 agar dapat menangani pelaku phishing secara tepat.[11]

Dalam sistem perbankan, scam link berbahaya telah menjadi salah satu ancaman siber yang semakin sering terjadi di Indonesia. Pemerintah telah memberlakukan berbagai aturan hukum untuk mengatasi tindak kejahatan ini, baik melalui undang-undang khusus mengenai kejahtan phishing elektronik perlindungan konsumen di bidang perbankan. Beberapa peraturan yang relevan dalam menangani kejahatan phishing antara lain adalah:[12]

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Perubahannya dalam Undang-Undang Nomor 19 Tahun 2016 merupakan dasar hukum utama dalam mengatur kegiatan di dunia maya, termasuk tindakan kejahatan yang disebut phishing. Dalam Pasal 28 ayat (1) UU ITE disebutkan bahwa setiap orang dilarang sengaja dan tanpa izin menyebarkan informasi elektronik yang dapat menyesatkan dan merugikan konsumen dalam transaksi elektronik. Selain itu, Pasal 35 UU ITE juga mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak memanipulasi, mengubah, atau membuat informasi elektronik atau dokumen elektronik agar terlihat seperti asli dapat dikenai ancaman hukuman.
2. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) UU PDP mengatur perlindungan data pribadi masyarakat agar tidak dimanfaatkan oleh pihak yang tidak bertanggung jawab. Kejahatan phishing sering kali melibatkan Pencurian data pribadi seperti nama, nomor rekening, dan kredensial login nasabah

[9] Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. PAMPAS: Journal of Criminal Law, 1(2), 68–81. https://doi.org/10.22437/pampas.v1i2.9574

[10] Wahyu Hidayat M, Hartini Ramli, Ikhram, P. M. B., Sidrayanti, Ridhawi, A. R., Mukhtar, N. A., & Renaldy Junedy. (2023). Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar. Vokatek : Jurnal Pengabdian Masyarakat, 1(1), 28–33

[11] Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO), 223–234

[12] Yustitiana, R. (2021). Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phishing Transaksi Elektronik Sebagai Bagian dari Upaya Penegakan Hukum di Indonesia Dikaitkan Dengan Teori Efektivitas Hukum. Jurnal Hukum Visio Justisia, 1(1), 98-126.

perbankan dapat dikenai sanksi pidana menurut undang-undang. Orang yang mengakses atau menggunakan data pribadi seseorang tanpa izin bisa dihukum.

3. Kitab Undang-Undang Hukum Pidana (KUHP) Meskipun KUHP tidak secara langsung mengatur tindak kejahatan siber, beberapa pasal dapat diterapkan dalam kasus phishing. Misalnya, Pasal 378 KUHP tentang penipuan dapat digunakan untuk menjerat pelaku yang sengaja mengelabui korban demi mendapatkan keuntungan tidak sah. Selain itu, Pasal 362 KUHP tentang pencurian juga dapat diterapkan jika tindakan phishing menyebabkan kerugian finansial pada korban.
4. Peraturan Bank Indonesia (PBI) dan Peraturan Otoritas Jasa Keuangan
   (OJK) Untuk melindungi nasabah dan menjaga keamanan transaksi digital, BI dan OJK memberikan aturan yang relevan.
5. PBI Nomor 22/20/PBI/2020 tentang Keamanan Sistem Pembayaran, yang mewajibkan bank dan penyedia layanan keuangan untuk menerapkan sistem keamanan yang ketat guna mencegah penyalahgunaan data nasabah.
6. POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, yang mengatur kewajiban lembaga keuangan memberikan edukasi dan perlindungan kepada nasabah terkait risiko kejahatan digital.
7. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UU PK) UU PK memberikan dasar hukum bagi nasabah yang mengalami kerugian karena tindakan phishing. Bank sebagai penyedia layanan perbankan wajib memastikan keamanan sistem dan memberi informasi yang jelas mengenai risiko transaksi daring. Jika bank tidak memberikan perlindungan yang memadai, nasabah yang mengalami kerugian dapat menuntut ganti rugi berdasarkan ketentuan dalam UU PK.

Sanksi Hukum bagi Pelaku Kejahatan Phishing di Indonesia sanksi yang diberikan kepada pelaku phishing dalam sistem perbankan digital melalui tautan penipuan berbahaya bisa berupa sanksi pidana atau perdata, tergantung pada dampak yang ditimbulkan kepada korban dan cara kejahatan tersebut dilakukan.

Beberapa ketentuan sanksi yang dapat diterapkan antara lain:[13]

1. Sanksi Pidana Berdasarkan UU ITE
   1) Pasal 28 ayat (1): Siapa saja yang menyebarkan informasi elektronik yang menyesatkan dan merugikan konsumen bisa dipidana dengan hukuman penjara paling lama 6 tahun dan/atau denda maksimal Rp1
   miliar.
   2) Pasal 35 dan Pasal 51 ayat (1): Siapa saja yang sengaja memanipulasi data elektronik agar terlihat sah bisa dipidana dengan hukuman penjara paling lama 12 tahun dan/atau denda maksimal Rp12 miliar.
2. Sanksi Pidana Berdasarkan UU PDP
   1) Pasal 67 dan Pasal 68: Siapa saja yang secara ilegal memperoleh, mengungkapkan, atau menggunakan data pribadi seseorang tanpa izin bisa dipidana dengan hukuman penjara paling lama 6 tahun dan/atau denda hingga Rp6 miliar.
3. Sanksi Pidana Berdasarkan KUHP
   1) Pasal 378 (Penipuan): Pelaku phishing yang terbukti melakukan penipuan bisa dikenakan hukuman penjara paling lama 4 tahun.
   2) Pasal 362 (Pencurian): Jika phishing menyebabkan kerugian finansial, pelaku bisa dikenai tuntutan pencurian dengan ancaman hukuman penjara paling lama 5 tahun.
   3) Sanksi Perdata Berdasarkan UU Perlindungan Konsumen
      a) Konsumen atau nasabah yang mengalami kerugian karena kelalaian bank dalam melindungi sistem perbankan digital bisa mengajukan gugatan ganti rugi berdasarkan Pasal 19 UU PK.
      b) Bank juga bisa dituntut jika terbukti tidak memberikan informasi yang cukup kepada nasabah terkait keamanan perbankan digital atau tidak menyediakan langkah mitigasi yang memadai terhadap risiko kejahatan phishing.

Dalam praktiknya, bank hanya bertanggung jawab atas tindakan atau kelalaian pegawainya jika terbukti ada keterlibatan atau instruksi dari pihak bank yang tidak sesuai. Bank bisa bertanggung jawab atas kerugian yang dialami nasabah akibat tindakan salah atau kelalaian pegawainya sesuai dengan peraturan yang berlaku. Jadi, dalam konteks tanggung jawab perdata, bank bertanggung jawab atas kerugian yang disebabkan oleh kesalahan atau kelalaian pegawainya berdasarkan hukum yang berlaku,

[13] Wiranata, G. A., Ucuk, Y., & Sidarta, D. D. (2024). Pertanggungjawaban Pidana terhadap Pelaku Tindak Pidana Phishing. Court Review: Jurnal Penelitian Hukum (e-ISSN: 2776-1916), 4(02), 13-25.

dan hal ini bisa dianggap sebagai tanggung jawab perusahaan bank.

Perlindungan hukum bagi pengguna layanan perbankan, sesuai dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan ("UU 10/1998"), mencakup beberapa hal yang penting bagi nasabah:[14]

1. Penyediaan informasi mengenai risiko kerugian: UU 10/1998 menyatakan bahwa bank wajib memberi informasi kepada nasabah mengenai kemungkinan risiko kerugian dari transaksi yang dilakukan. Hal ini bertujuan agar nasabah mendapat informasi yang jelas dan transparan tentang kondisi keuangan bank dan risiko yang bisa diterima.
2. Rahasia bank: UU 10/1998 melindungi rahasia bank, meliputi informasi tentang nasabah dan tabungannya. Bank harus menjaga kerahasiaan ini, kecuali dalam situasi yang diatur oleh undang-undang, seperti kepentingan perpajakan, proses hukum, atau atas persetujuan nasabah secara tertulis.
3. Lembaga Penjamin Simpanan: UU 10/1998 mewajibkan setiap bank menjamin dana masyarakat yang disimpan. Hal ini diimplementasikan melalui Lembaga Penjamin Simpanan (LPS) yang bertugas memberi jaminan atas tabungan nasabah jika bank mengalami kesulitan keuangan.

Selain ketiga hal tersebut, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen ("UU 8/1999") juga memberikan perlindungan tambahan kepada nasabah perbankan. UU ini menetapkan standar perilaku yang harus diikuti oleh lembaga jasa perbankan, termasuk kewajiban untuk memberikan informasi yang jujur, tidak diskriminatif, serta melindungi nasabah dari klausula baku yang merugikan.

Nasabah bisa menggugat bank jika ada kasus phising dan bank dianggap tidak melindungi data atau sistem keamanannya dengan baik, sehingga mudah disusupi. Pertanggungjawaban ini biasanya memerlukan bukti bahwa bank tidak menerapkan protokol keamanan yang cukup atau gagal memberi informasi kepada nasabah mengenai bahaya phising. Bank wajib menggunakan teknologi antiphising yang bisa mengurangi serangan siber, serta secara rutin mengajarkan nasabah cara menghindari jebakan phising. Contohnya adalah kampanye digital, peringatan, dan panduan keamanan di aplikasi serta situs web bank. Dengan langkah-langkah ini, bank menunjukkan bahwa mereka sudah berusaha mencegah pelanggaran siber dan melindungi nasabah mereka. Bank sangat bertanggung jawab dalam melindungi data nasabah, terutama karena layanan mobile banking semakin populer. Berdasarkan Pasal 29 Undang-Undang No 21 Tahun 2011 tentang Otoritas Jasa Keuangan, bank bertanggung jawab memastikan informasi nasabah tetap aman. Bank harus mengaplikasikan teknologi seperti autentikasi berlapis, enkripsi data, dan notifikasi keamanan untuk mengenali aktivitas mencurigakan, sehingga dapat melindungi data nasabah mereka.[15]

Meskipun begitu, masih diperlukan penyesuaian lebih lanjut melalui peraturan pemerintah, terutama terkait dengan syarat minimum sistem elektronik yang harus dipenuhi. Dalam konteks melindungi nasabah yang menjadi korban pencurian data, bank wajib melakukan upaya pencegahan yang tepat, seperti memverifikasi identitas pengguna layanan perbankan dan bekerja sama dengan lembaga penegak hukum sesuai dengan ketentuan mengenai kerahasiaan bank.

Perlindungan bagi nasabah bank dapat dilakukan dengan dua cara, yaitu secara implisit dan eksplisit:

1) Perlindungan secara implisit melibatkan pengawasan dan pembinaan yang efektif untuk mencegah bank bangkrut. Hal ini dapat dicapai melalui regulasi perbankan, pengawasan dari Bank Indonesia, menjaga kesehatan bank, serta memberi informasi risiko kepada bank.
2) Perlindungan secara eksplisit dilakukan dengan membuat lembaga yang menjamin uang tabungan masyarakat. Jika bank mengalami kegagalan, lembaga tersebut akan mengganti uang nasabah.

Selain itu, untuk memberi perlindungan hukum kepada dana nasabah, bank melakukan beberapa langkah seperti:[16]

a) Menggunakan teknologi Secure Socket Layer (SSL) atau bisa disebut enkripsi 128 bit untuk melindungi komunikasi antara komputer nasabah dan server bank. Akses ke server bank otomatis ditutup setelah periode tidak aktif tertentu.

[14] Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan

[15] Alfred Yetno, 2024, "Tanggung Jawab Bank Dalam Menjaga Keamanan dan Kerahasiaan Data NasabahPerbankan di Indonesia" 10, no. 1 : 67–76. Kata Kunci dan Keamanan Kerahasiaan.

[16] Jefry Tarantang dkk, 2023, Perlindungan Hukum Terhadap Nasabah Bank Dalam Transaksi Digital. Morality: Jurnal Ilmu Hukum, no.1:19 http://dx.doi.org/10.52947/morality.v9i1.321

b) Memastikan kerahasiaan data nasabah dan hanya orang yang berwenang yang bisa mengaksesnya.
c) Tidak mengumpulkan informasi data pengguna internet banking secara otomatis, melainkan hanya informasi umum seperti domain dan jenis browser.
d) Nasabah wajib memasukkan user ID dan PIN untuk mengakses layanan internet banking, serta memasukkan kembali PIN untuk melakukan transaksi keuangan.
e) Bank menyediakan layanan internet banking yang sesuai dengan standar browser tertentu seperti Netscape Communicator 4.7 atau Microsoft Internet Explorer 5.01.

Dengan langkah-langkah tersebut, upaya untuk melindungi dana nasabah sudah dilakukan, termasuk perlindungan data pribadi dan syarat ketat untuk bertransaksi lewat layanan internet banking. Meskipun demikian, ancaman kejahatan cybercrime masih ada dan perlu tetap diwaspadai.

**B. Pelaksanaan Perlindungan Hukum Bank Terhadap Nasabah Korban Phishing**

Kepercayaan nasabah sangat penting bagi perbankan. Phishing adalah salah satu jenis kejahatan yang bisa membahayakan keamanan dana nasabah di industri perbankan. Selain itu, upaya bank untuk menjaga reputasinya dan mendapatkan kepercayaan nasabah bisa terganggu karena risiko keamanan ini. Hubungan yang baik antara bank dan nasabah bergantung pada rasa aman dan kepercayaan yang mereka miliki. Oleh karena itu, bank harus melakukan langkah-langkah untuk mencegah dan mengatasi phishing agar keamanan nasabah tetap terjaga dan risiko yang mungkin terjadi bisa diminimalkan. Memastikan keamanan membutuhkan penerapan teknologi terkini, sikap transparan, serta mengajarkan para nasabah.[17]

Bank mengatakan bahwa serangan phishing juga bisa terjadi karena kelalaian dari nasabah, seperti tindakan yang membuat celah bagi pelaku phishing. Bank menyarankan agar dalam menentukan tanggung jawab secara ketat, agar mencegah terulangnya laporan serupa dan memastikan proses pengaduan berjalan lancar, nasabah yang mengajukan pengaduan tidak mengulang laporan lebih dari satu kali. Jika hasil penyelidikan menunjukkan bahwa serangan phishing tersebut disebabkan oleh kecerobohan nasabah, maka nasabah bertanggung jawab penuh. Karena dianggap berada di luar kendali bank, maka bank tidak memberikan ganti rugi kepada nasabah. Menurut Undang-Undang No 19 Tahun 2016 tentang ITE, persepsi nasabah terhadap keamanan dan kenyamanan layanan perbankan digital, seperti mobile banking,[18] juga dipengaruhi pelanggan juga memiliki tanggung jawab untuk menjaga keamanan data mereka dan menghindari mengungkapkan informasi sensitif kepada pihak yang tidak bertanggung jawab. Menurut Pasal 26 UUITE (Informasi dan Transaksi Elektronik), pelanggan memiliki alasan hukum untuk tidak membayar kerugian jika mereka membuat kesalahan atau tidak menginformasikan data mereka kepada pihak yang tidak bertanggung jawab.

Perlindungan terhadap nasabah sangat penting karena ada risiko yang bisa terjadi kepada mereka. Perlindungan data nasabah di bank Indonesia bisa dilakukan dengan dua cara yakni:[19]

1) Perlindungan secara eksplisit, yaitu perlindungan yang dilakukan dengan cara membuat suatu lembaga bernama Lembaga Penjamin Simpanan (LPS). Lembaga ini dibuat berdasarkan Keputusan Presiden RI Nomor 26 Tahun 1998 mengenai Jaminan Terhadap Kewajiban Umum serta Undang-Undang Nomor 24 Tahun 2004 tentang LPS. LPS berfungsi sebagai penjamin uang yang disimpan oleh nasabah di bank. Jika suatu bank mengalami gagal, LPS akan mengganti uang nasabah tersebut. Selain itu, LPS juga aktif dalam menjaga kestabilan sistem perbankan sesuai dengan kewenangannya.
2) Perlindungan secara implisit, yaitu penerapan pengawasan serta pembinaan terhadap bank sebagai bentuk perlindungan yang efektif untuk mencegah terjadinya kebangkrutan bank. Perlindungan implisit ini, ada beberapa upaya yakni perlindungan melalui peraturan perundang-undangan di bidang perbankan; pengawasan dan pengarahan yang efisien oleh Bank Indonesia dengan memantau kinerja bank dalam melindungi nasabah serta memberikan bimbingan kepada bank yang tidak sehat menjaga kelangsungan usaha bank sebagai lembaga serta perlindungan terhadap sistem perbankan secara umum menjaga kesehatan bank melalui pembinaan yang dilakukan Bank Indonesia penerapan prinsip

[17] "PT BRI Multifinance Indonesia," 2023.

[18] Kadek Yogi Pratama Putra, A Agung Sagung Laksmi Dewi, and Luh Putu Suryani, 2021 "Perlindungan HukumKorbanPenipuan Undian Berhadiah sesuai UU No 11 Tahun 2008 mengenai Informasi juga Transaksi Elektronik," Jurnal Interpretasi Hukum 2, no.3: 673–77, https://doi.org/10.22225/juinhum.2.3.4195.673-677.

[19] Kinot, I. R., Adji, H. S., Setiawan, R., & Harianto, A. (2022). Perlindungan Hukum Terhadap Nasabah Penyimpan Dana Di Bank Oleh Lembaga Penjamin Simpanan. Jurnal Yustisiabel, 6(1), 110-131.

kehati-hatian sesuai ketentuan Pasal 2 Undang-Undang

Kitab Undang-Undang Hukum Pidana (KUHP) juga dapat digunakan melalui Pasal 378 (penipuan) dan Pasal 362 (pencurian), tetapi bukti digital yang diperlukan sering kali sulit dikumpulkan, menyebabkan proses peradilan yang panjang dan mahal bagi korban.[20]

Hasil penelitian menunjukkan bahwa regulasi di Indonesia telah mengatur sanksi bagi pelaku, tetapi tantangan dalam implementasi hukum tetap ada, seperti kesulitan pembuktian dan penegakan oleh aparat penegak hukum.

Selain itu, Undang-Undang Perbankan (UU No. 10/1998) menekankan kerahasiaan data nasabah (Pasal 1 angka 28), tetapi tidak secara eksplisit mengatur mekanisme ganti rugi bagi korban phishing yang disebabkan oleh kelalaian bank.

Salah satu kendala utama dalam pelaksanaan perlindungan hukum adalah ketidakjelasan dan fragmentasi regulasi yang ada. UU ITE, meskipun mengatur penyalahgunaan transaksi elektronik (Pasal 28-32), belum secara eksplisit mendefinisikan phishing sebagai kejahatan siber yang terpisah, sehingga sulit diterapkan secara konsisten. Hal ini menyebabkan korban sering kali dianggap lalai (negligent) karena "tertipu" oleh taktik social engineering, seperti email palsu atau situs web tiruan, tanpa mekanisme yang jelas untuk membebankan tanggung jawab pada bank. Selain itu, regulasi seperti POJK Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen Sektor Jasa Keuangan menekankan prinsip kerahasiaan data (Pasal 29 ayat 4 UU Perbankan), tetapi implementasinya bergantung pada bukti yang kuat dari nasabah, yang sering kali sulit diperoleh karena sifat transaksional phishing yang cepat dan lintas yurisdiksi.

Fragmentasi regulasi juga terlihat dari kurangnya koordinasi antarlembaga, seperti antara Otoritas Jasa Keuangan (OJK), Bank Indonesia (BI), dan Kementerian Komunikasi dan Informatika (Kominfo). Misalnya, POJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi mewajibkan bank untuk menerapkan sistem keamanan, tetapi tidak ada sanksi tegas jika terjadi kebocoran data akibat phishing, yang sering kali dieksploitasi oleh pelaku di luar negeri. Akibatnya, perlindungan hukum cenderung reaktif daripada preventif, di mana nasabah harus melalui proses pengaduan panjang ke Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK), yang memakan waktu dan biaya.[21]

Penegakan hukum terhadap kasus phishing menghadapi tantangan signifikan, terutama karena kurangnya pemahaman teknologi di kalangan penegak hukum. Seperti yang diungkapkan dalam studi di Polda Jawa Timur, penyidik sering kesulitan melacak pelaku karena keterbatasan anggaran, kurangnya keterampilan digital, dan resistensi terhadap perubahan teknologi. Phishing sering melibatkan domain palsu (seperti kasus klikbca.com pada 2001 terhadap Bank BCA) yang diselenggarakan di server luar negeri, sehingga memerlukan kerjasama internasional yang lambat.

Selain itu, distribusi infrastruktur teknologi yang tidak merata di daerah pedesaan memperburuk masalah, di mana nasabah kurang teredukasi tentang risiko, sementara pelaku memanfaatkan faktor sosial-ekonomi seperti rendahnya literasi digital. Studi kasus di PT Bank Rakyat Indonesia (BRI) menunjukkan bahwa meskipun bank menerapkan prinsip kerahasiaan, penegakan hukum terhadap pelaku phishing masih bergantung pada laporan nasabah, yang sering terlambat karena korban enggan melapor akibat stigma atau ketakutan. Akibatnya, tingkat konversi kasus dari laporan ke vonis rendah, dengan hanya sebagian kecil pelaku yang tertangkap, sehingga mengurangi efek jera dan kepercayaan nasabah terhadap sistem perbankan.[22]

Kendala dari sisi nasabah meliputi rendahnya literasi digital, di mana banyak korban phishing jatuh ke dalam jebakan karena kurangnya kesadaran akan modus seperti SMS undian palsu atau chat palsu. Hal ini membuat bank sulit memberikan perlindungan penuh, karena tanggung jawab sering dibagi antara bank dan nasabah. Dari sisi bank, kendala institusional termasuk keterbatasan sumber daya untuk edukasi masif dan penanganan klaim ganti rugi yang cepat. Kendala ini menciptakan siklus di mana nasabah menyalahkan bank, sementara bank menyalahkan kelalaian nasabah, sehingga proses pengaduan menjadi panjang. Edukasi melalui media sosial dan simulasi diperlukan untuk membangun kewaspadaan, tetapi tantangan akses internet di Indonesia memperburuk situasi. Penelitian menekankan bahwa bank berkewajiban secara preventif melalui edukasi, tetapi

[20] Sitorus, R., Saragih, J. Z. F., & Banke, R. (2025). Kendala Pelaksanaan Perlindungan Data Pribadi. Locus: Jurnal Konsep Ilmu Hukum, 5(1), 53-61.

[21] Ekawati, D., Herdiana, D., & Haryanti, A. (2025). Phishing in the Banking Sector: Between Cybercrime and Consumer Protection. SIGn Jurnal Hukum, 7(1), 133-151.

[22] Rahmana, R. D., & Kartika, A. W. (2022). Penegakan Hukum Bagi Pelaku Pembuatan Dan Penyebaran Scam Page (Studi Di Kepolisian Daerah Jawa Timur). risalah hukum, 18(2), 8398.

implementasinya belum merata, terutama di daerah pedesaan.[23]

Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) memiliki peran dalam mengawasi, tetapi kendala koordinasi antar lembaga sering menghambat penegakan. Selain itu, proses litigasi bagi nasabah korban sering kali mahal dan memakan waktu, sehingga banyak kasus tidak dilaporkan.

Bank BRI, sebagai Badan Usaha Milik Negara (BUMN) yang beroperasi di bidang perbankan dengan pengalaman lebih dari 120 tahun, memiliki komitmen untuk memberikan kemudahan dan respons cepat terhadap berbagai kebutuhan nasabah. BRI Mobile atau BRImo adalah aplikasi terbaru dari Bank BRI yang berbasis pada konektivitas internet, dirancang untuk memberikan kemudahan bagi para nasabah. Aplikasi ini dilengkapi dengan fitur canggih seperti login menggunakan pengenalan wajah dan sidik jari, memungkinkan pengisian saldo

Dalam menjalankan layanan perbankannya, BRI menerapkan prinsip perlindungan konsumen. Hal ini mencakup tanggung jawab untuk melindungi nasabah secara preventif dan represif. Tanggung jawab preventif BRI adalah dengan adanya prosedur yang dirancang untuk mencegah terjadinya phishing. Salah satu prosedur tersebut adalah meningkatkan pengetahuan nasabah mengenai ancaman phishing dan cara melindungi diri dari serangan tersebut. Tanggung jawab represif diberikan kepada nasabah yang sudah terkena serangan phishing. Ini mencakup langkah-langkah untuk menangani dan menyelesaikan masalah yang terjadi setelah serangan phishing.[24]

Tanggung jawab BRI dalam bentuk perlindungan preventif antara lain adalah menggunakan media sosial, khususnya Twitter, dan pesan email untuk secara berkala menginformasikan nasabah tentang keamanan transaksi e-banking. Hal ini mencerminkan upaya bank untuk meningkatkan kesadaran nasabah tentang ancaman keamanan dan memberikan panduan transaksi yang aman. Selain itu, BRI tidak membatasi nasabah yang memiliki kekhawatiran terkait e-banking, tetapi tetap memberikan ruang, waktu, dan kesempatan untuk berbicara langsung. Ini menciptakan saluran komunikasi terbuka antara bank dan nasabah untuk menanggapi kekhawatiran atau pertanyaan secara langsung. Dalam menjalankan layanan operasional perbankan, BRI melakukan manajemen risiko secara komprehensif dalam seluruh layanan operasionalnya. Ini mencakup penggunaan metodologi dan efektivitas aktivitas manajemen risiko secara berkala sesuai dengan ketentuan Kebijakan Umum Manajemen Risiko. Hal ini mengingat perkembangan teknologi dan kemunculan e-banking, sehingga diperlukan pengelolaan yang baik dalam mengendalikan risiko teknologi informasi. Ini mencakup arahan dan pengendalian yang diperlukan dalam menjalankan manajemen risiko terkait teknologi informasi. Secara keseluruhan, BRI memiliki pendekatan untuk melindungi nasabah terhadap ancaman phishing dan mengelola risiko operasional terkait teknologi informasi.[25]

BRI menjelaskan bahwa kelalaian nasabah juga bisa menjadi penyebab dari serangan phishing. Ini mencakup tindakan yang mungkin dilakukan nasabah, seperti membuka celah `bagi orang-orang yang ingin melakukan serangan phishing.

Dalam proses memberikan tanggung jawab secara represif, BRI memberikan himbauan agar nasabah yang mengadukan masalah tidak menyampaikan laporan berulang kali. Hal ini dilakukan untuk mencegah pengulangan laporan yang sama dan memastikan proses penanganan pengaduan menjadi lebih efisien. Jika selama proses penyelidikan ditemukan bahwa kejadian phishing disebabkan oleh kelalaian nasabah, maka nasabah tersebut harus bertanggung jawab penuh. Karena itu, bank tidak memberikan ganti rugi kepada nasabah karena dianggap bukan kesalahan dari pihak bank.

UU No. 19 Tahun 2016 tentang ITE memiliki dampak terhadap persepsi nasabah terkait rasa aman dan nyaman dalam menggunakan layanan perbankan digital, seperti e-banking. Hal ini dikarenakan dalam undang-undang tersebut dijelaskan bahwa bank memiliki tanggung jawab secara hukum apabila terjadi kerugian pada nasabah yang menggunakan layanan dari bank tersebut. Namun, jika kerugian disebabkan oleh nasabah itu sendiri, seperti kelalaian atau keadaan force majeure, maka bank tidak bertanggung jawab. Dengan demikian, BRI melakukan pendekatan yang seimbang antara memberikan perlindungan kepada nasabah dan menegakkan tanggung jawab nasabah dalam upaya mencegah serangan phishing.[26] BRI memiliki tanggung

[23] Ekayani, L., Djanggih, H., & Suong, M. A. A. (2023). Perlindungan hukum nasabah terhadap kejahatan pencurian data pribadi (phising) di lingkungan perbankan. Journal of Lex Philosophy (JLP), 4(1), 22-40.

[24] Sianipar, J. J., & Naibaho, M. S. (2024). LEMAHNYA KEAMANAN BANK PEMERINTAH DI INDONESIA: STUDI KASUS PERETASAN BANK BRI TERHADAP NASABAHNYA. Jurnal Multidisiplin Ilmu Akademik, 1(6), 236-241.

[25] PT. BRI Multifinance Indonesia. (2022).Kebijakan Manajemen Risiko. BRI Finance.

[26] Putra, K. Y. P., Dewi, A. A. S. L., & Suryani, L. P. (2021). Perlindungan Hukum Korban Penipuan Undian Berhadiah

jawab untuk menangani kasus phising secara represif. Salah satu hak nasabah adalah menggugat BRI ke pengadilan jika penyelesaian yang ditawarkan oleh bank tidak memenuhi harapan. Gugatan ini bisa diajukan karena BRI dianggap bertanggung jawab atas kerugian yang dialami nasabah akibat serangan phising dalam penggunaan sistem e-banking. Selain menggugat ke pengadilan, nasabah juga bisa meminta bantuan OJK. OJK dapat membantu mempercepat proses pengaduan dan menyelesaikan masalah yang dialami nasabah. Langkah ini menunjukkan adanya mekanisme penyelesaian sengketa di luar pengadilan. Namun, BRI berusaha memilih penyelesaian secara damai dengan berbagai cara seperti negosiasi, mediasi, atau penyelesaian di luar pengadilan. Upaya damai dilakukan untuk menjaga hubungan baik dengan nasabah dan menghindari dampak negatif terhadap reputasi bank. Reputasi dan kepercayaan nasabah dianggap sangat penting dalam menangani kasus phising. BRI berupaya menjaga kepercayaan nasabah dengan menawarkan penyelesaian yang memadai dan menghindari proses pengadilan yang bisa merugikan hubungan tersebut.[27]

Bank wajib mengamankan dan merahasiakan data nasabah secara hukum. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan melindungi dana nasabah, tetapi perlindungan data nasabah masih perlu diperhatikan lebih lanjut.

## PENUTUP

### A. Kesimpulan

1. Berdasarkan hasil penelitian, dapat disimpulkan bahwa perlindungan hukum terhadap dana nasabah bank dari serangan phishing diatur secara cukup komprehensif melalui berbagai peraturan perundang-undangan, seperti UndangUndang Perlindungan Konsumen, Undang-Undang Informasi dan Transaksi Elektronik, serta regulasi dari Otoritas Jasa Keuangan (OJK). Peraturan tersebut mengatur kewajiban bank untuk menjaga keamanan data dan transaksi nasabah, serta memberikan perlindungan hukum terhadap nasabah yang menjadi korban phishing. Meskipun demikian, implementasi dan penegakan peraturan ini masih memerlukan perhatian agar perlindungan hukum dapat berjalan efektif dan menjamin hak-hak nasabah secara maksimal.
2. Pelaksanaan perlindungan hukum bank terhadap nasabah korban phishing di Indonesia yaitu regulasi yang masih bersifat umum dan kurang spesifik terhadap kasus phishing, seperti yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta regulasi Otoritas Jasa Keuangan (OJK), yang sering kali tidak menjangkau aspek tanggung jawab bank secara detail. Selain itu, keterbatasan teknologi keamanan di sistem perbankan, kurangnya koordinasi antara bank dengan aparat penegak hukum, serta rendahnya literasi digital nasabah menjadi faktor penghambat utama dalam penanganan kasus. Meskipun bank memiliki tanggung jawab hukum untuk melindungi nasabah melalui upaya preventif dan represif, implementasi di lapangan sering terhambat oleh prosedur klaim yang rumit dan kurangnya bukti digital yang kuat. Secara keseluruhan, kendala ini mengakibatkan nasabah korban phishing sering mengalami kerugian finansial tanpa kompensasi yang memadai, sehingga diperlukan reformasi untuk meningkatkan efektivitas perlindungan hukum.

### B. Saran

1. Teknologi keamanan harus terus dikembangkan, seperti autentikasi dua faktor dan enkripsi data, guna menghadapi semakin canggihnya serangan phishing. Regulasi pun perlu diperbarui secara berkala agar tetap relevan dan mampu melindungi terhadap risiko yang berkembang. Pengawasan yang ketat dari otoritas juga penting untuk memastikan penerapan aturan berjalan efektif dan konsisten. Selain itu, penelitian lanjutan diperlukan untuk menilai efektivitas perlindungan dan mencari solusi inovatif dalam menghadapi ancaman siber. Dengan langkah ini, perlindungan hukum terhadap dana nasabah dapat terus diperkuat dan beradaptasi dengan perkembangan teknologi.
2. Untuk perlindungan hukum bank terhadap nasabah korban phishing, pemerintah melalui OJK dan Kementerian Hukum dan HAM perlu menyusun regulasi khusus yang tegas mengatur tanggung jawab bank serta mekanisme kompensasi cepat, termasuk amandemen UU ITE agar lebih responsif terhadap perkembangan teknologi siber. Bank juga diharapkan meningkatkan keamanan sistem melalui pemantauan transaksi real-time, dan kerja sama dengan penyedia

Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Jurnal Interpretasi Hukum, 2(3)

[27] Indonesia, I. B. (2016). Strategi Manajemen Risiko . Gramedia Pustaka Utama.

cybersecurity untuk mencegah serangan phishing. Di sisi lain, edukasi rutin bagi nasabah melalui kampanye media sosial, seminar, dan fitur di aplikasi perbankan menjadi langkah penting guna meningkatkan literasi digital dan mengurangi risiko korban. Koordinasi antar lembaga antara bank, polisi siber, dan peradilan perlu diperkuat melalui tim khusus atau platform berbagi data demi mempercepat investigasi dan penegakan hukum. Selain itu, penelitian lanjutan dengan analisis kasus empiris dan perbandingan internasional, seperti di Singapura atau Eropa, diperlukan untuk mengadopsi praktik terbaik. Implementasi menyeluruh dari langkah-langkah ini akan membuat perlindungan hukum bank terhadap nasabah korban phishing jauh lebih efektif dan responsif di masa mendatang.

## DAFTAR PUSTAKA

**Buku**

Abdurrachman, 2014. Ensiklopedia Ekonomi Keuangan Perbankan, PT. Pradya Paramitya. Jakarta.

CST Kansil, 1980, Pengantar Ilmu Hukum dan Tata Hukum Indonesia, Balai Pustaka, Jakarta

Hermansyah, 2008. Hukum Perbankan Nasional Indonesia, Prenada Media Group, Jakarta.

Kasmir, 2012. Dasar – Dasar Perbankan, Depok: RajawaliPers.

Ketut Rindjin, 2012. Pengantar Perbankan dan Lembaga Keuangan Bukan Bank, Jakarta : Gramedia Pustaka Utama.

Kuncoro, Mudrajad dan Suhardjono, 2010. Manajemen Perbankan, Teori dan Aplikasi, Yogyakarta: BPFE.

Maryanto, 2011. Buku Pintar Perbankan, (Yogyakarta: Andi Offset.)

Muchsin, 2013, Perlindungan dan Kepastian Hukum bagi Investor di Indonesia, Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret, Surakarta.

Nasution, M. Nur. 2004. ManajemenJasa Terpadu. Bogor: Ghalia Indonesia.

Peter Mahmud Marzuki, 2011, "Penelitian Hukum", Prenada Media Grup, Jakarta.

Phillipus M. Hadjon, 1987, Perlindungan Hukum Bagi Rakyat Indonesia, PT. Bina Ilmu, Surabaya.

Ricardi Hermawan, 2009. The Drop Out Billionaire Menjual Ide Ala Mark

Zuckerberg, Best Publisher, Yogyakarta.

Sembiring Sentosa. 2012. Hukum Perbankan. Edisi Revisi. Bandung : Mandar Maju.

Setiono, 2004, Rule of Law (Supremasi Hukum), Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret, Surakarta.

Soerjono Soekanto, 1986, "Pengantar Penelitian Hukum", UI-Press, Jakarta.

Uswatun Hasanah, 2017. 'Hukum Perbankan' (Setara Press).

Widjanarto, 2003. Hukum dan Ketentuan Perbankan di Indonesia, Jakrta: Grafiti.

Yusuf Shofie, 2000. Perlindungan Konsumen, Bandung: Citra Aditya Bakti.

Yusuf Shofie, 2003. Perlindungan Konsumen dan Instrumen-Instrumen Hukumnya, (Citra Aditya BaktiBandung).

**Jurnal**

Alfred Yetno, 2024, "Tanggung Jawab Bank Dalam Menjaga Keamanan dan Kerahasiaan Data NasabahPerbankan di Indonesia" 10, no. 1 : 67–76. Kata Kunci dan Keamanan Kerahasiaan.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. Prosiding Seminar

Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO), 223–234

Ekawati, D., Herdiana, D., & Haryanti, A. (2025). Phishing in the Banking Sector: Between Cybercrime and Consumer Protection. SIGn Jurnal Hukum, 7(1), 133-151.

Fadiah Azzahra Gusti, 'Kelalaian Bank Dalam Menjaga Rahasia Bank Pada Perjanjian Baku Terhadap Tindakan Phising Yang Dialami Nasabah Akibat Social Engineering Ditinjau Dari Hukum Positif Indonesia', Jurnal MAHUPAS: Mahasiswa Hukum Unpas, 2.2 (2023), pp. 1–18.

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. PAMPAS: Journal of Criminal Law, 1(2), 68–81.

Hardi Fardiansyah,(Et.Al.), Cyber Crime Paling Populer Pada Era Digital, Media Sains Indonesia, Bandung, (2022).

Rahmana, R. D., & Kartika, A. W. (2022). Penegakan Hukum Bagi Pelaku Pembuatan Dan Penyebaran Scam Page (Studi Di Kepolisian Daerah Jawa Timur). risalah hukum, 18(2), 83-98.

Jefry Tarantang dkk, 2023, Perlindungan Hukum Terhadap Nasabah Bank Dalam Transaksi Digital. Morality : Jurnal Ilmu Hukum, no.1:19 http://dx.doi.org/10.52947/morality.v9i1.321

Kadek Yogi Pratama Putra, A Agung Sagung Laksmi Dewi, and Luh Putu Suryani, 2021 "Perlindungan HukumKorbanPenipuan Undian Berhadiah sesuai UU No 11 Tahun 2008 mengenai Informasi juga Transaksi Elektronik," Jurnal Interpretasi Hukum 2, no.3: 673–77, https://doi.org/10.22225/juinhum.2.3.4195.673-677.

Kinot, I. R., Adji, H. S., Setiawan, R., & Harianto, A. (2022). Perlindungan Hukum Terhadap Nasabah Penyimpan Dana Di Bank Oleh Lembaga Penjamin Simpanan. Jurnal Yustisiabel, 6(1), 110

Moho, H., Ndruru, A., & Laowo, Y. (2023). Analisis Hukum Terhadap Perlindungan Dana Nasabah Pada Bank. Jurnal Panah Keadilan, 2(2), 8-15

Putra, K. Y. P., Dewi, A. A. S. L., & Suryani, L. P. (2021). Perlindungan Hukum Korban Penipuan Undian Berhadiah Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Jurnal Interpretasi Hukum, 2(3)

Siti Fatimah, 'Tinjauan Yuridis Terhadap Pelaku Tindak Pidana Perjudian Online Di Indonesia', Innovative: Journal Of Social Science Research, 3.2 (2023), pp. 3224–31.

Sitorus, R., Saragih, J. Z. F., & Banke, R. (2025). Kendala Pelaksanaan Perlindungan Data Pribadi. Locus: Jurnal Konsep Ilmu Hukum, 5(1), 53-61.

Slamet. (2022). Pertahanan Pencegahan Serangan Social Engineering Menggunakan Two Factor Authentication (2fa) Berbasis Sms (Short Message System). Nopember(Vol. 14)

Tyas Darmaningrat, E. W., Noor Ali, A. H., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D.. Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi.Sewagati,6(2). (2022).

Wahyu Hidayat M, Hartini Ramli, Ikhram, P. M. B., Sidrayanti, Ridhawi, A. R., Mukhtar, N. A., & Renaldy Junedy. (2023). Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar. Vokatek : Jurnal Pengabdian Masyarakat, 1(1), 28–33

Wiranata, G. A., Ucuk, Y., & Sidarta, D. D. (2024). Pertanggungjawaban Pidana terhadap Pelaku Tindak Pidana Phishing. Court Review: Jurnal Penelitian Hukum (e-ISSN: 2776-1916), 4(02), 13-25.

Yustitiana, R. (2021). Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phishing Transaksi Elektronik Sebagai Bagian dari Upaya Penegakan Hukum di Indonesia Dikaitkan Dengan Teori Efektivitas Hukum. Jurnal Hukum Visio Justisia, 1(1), 98-126.

Yosefine, Y., Agustina, R. S., & Agus, D. (2023). Perlindungan Hukum terhadap Nasabah BTPN Jenius akibat Tindakan Phishing (Studi Kasus Bank Tabungan Pensiunan Nasional Jenius). Yustisia Tirtayasa: Jurnal Tugas Akhir, 3(1), 57-72.

**Perundang-undangan**

Undang Undang No.10 Tahun 1998. Tentang Perbankan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

Peraturan Otoritas Jasa Keuangan Nomor 6/POJK.07/2022 Tahun 2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan

Peraturan Bank Indonesia Nomor 10/10/PBI/2008 Tahun 2008 tentang Penyelesaian Pengaduan Nasabah