PERLINDUNGAN HUKUM TERHADAP NASABAH KORBAN *PHISHING* DALAM SISTEM *E-BANKING* DI INDONESIA

SKRIPSI

Oleh:

Sofia Widiatul Hasana
NIM: 214102020029

UNIVERSITAS ISLAM NEGERI
KIAI HAJI ACHMAD SIDDIQ JEMBER
FAKULTAS SYARIAH
DESEMBER 2025

PERLINDUNGAN HUKUM TERHADAP NASABAH KORBAN *PHISHING* DALAM SISTEM *E-BANKING* DI INDONESIA

SKRIPSI

Diajukan kepada Universitas Islam Negeri
Kiai Haji Achmad Siddiq Jember
Untuk memenuhi salah satu persyaratan memperoleh
Gelar Sarjana Hukum (S.H.)
Fakultas Syariah
Program Studi Hukum Ekonomi Syariah

Oleh :

Sofia Widiatul Hasana
NIM: 214102020029

UNIVERSITAS ISLAM NEGERI
KIAI HAJI ACHMAD SIDDIQ JEMBER
FAKULTAS SYARIAH
DESEMBER 2025

PERLINDUNGAN HUKUM TERHADAP NASABAH KORBAN *PHISHING* DALAM SISTEM *E-BANKING* DI INDONESIA

SKRIPSI

Diajukan kepada Universitas Islam Negeri
Kiai Haji Achmad Siddiq Jember
Untuk memenuhi salah satu persyaratan memperoleh
Gelar Sarjana Hukum (S.H.)
Fakultas Syariah
Program Studi Hukum Ekonomi Syariah

Oleh:

Sofia Widiatul Hasana
NIM: 214102020029

Disetujui Pembimbing

Dr. H. Martoyo, S.H.I., M.H.
NIP. 197812122009101001

PERLINDUNGAN HUKUM TERHADAP NASABAH KORBAN *PHISHING* DALAM SISTEM *E-BANKING* DI INDONESIA

SKRIPSI

Telah diuji dan diterima untuk memenuhi salah satu
persyaratan memperoleh Gelar Sarjana Hukum (S.H)
Fakultas Syariah
Program Studi Hukum Ekonomi Syariah

Hari : Rabu
Tanggal : 17 Desember 2025

Tim Penguji

Ketua Sidang	**Sekretaris Sidang**
Freddy Hidayat, M.H.	**Afrik Yunari, M.H.**
NIP. 198808262019031003	**NIP. 199201132020122001**

Anggota :

1. Rumawi, S.H.I., M.H. ( )
2. Dr. H. Martoyo, S.H.I., M.H. ( )

Menyetujui
Dekan Fakultas Syariah

Dr. Wildani Hefni, M.A.
NIP . 19911107 201801 1 004

MOTTO

اِنَّ اللّٰهَ يَأْمُرُ بِالْعَدْلِ وَالْاِحْسَانِ وَاِيْتَاۤئِ ذِى الْقُرْبٰى وَيَنْهٰى عَنِ الْفَحْشَاۤءِ وَالْمُنْكَرِ وَالْبَغْيِ يَعِظُكُمْ لَعَلَّكُمْ تَذَكَّرُوْنَ ۝

Artinya: "Sesungguhnya Allah menyuruh (kamu) Berlaku adil dan berbuat kebajikan, memberi kertinya: pada kaum kerabat, dan Allah melarang dari perbuatan keji, kemungkaran dan permusuhan. Dia memberi pengajaran kepadamu agar kamu dapat mengambil pelajaran." (Q.S AN-NAHL:90)[*]

[*] Kementerian Republik Indonesia, *Al-Quran dan Terjemahannya*, (Semarang: Toha Putra, 2011)

PERSEMBAHAN

Puji syukur Alhamdulillah peneliti panjatkan atas rahmat dan karunianya, sehingga peneliti dapat menyelesaikan tugas akhir untuk memperoleh gelar sarjana hukum. Terima kasih banyak kepada orang-orang yang saya cinta dan sayangi, tidak lupa pula kepada orang-orang yang turut serta mendukung dalam proses penelitian karya tulis ini yaitu diantaranya:

1. Kepada cinta pertama dan panutanku, bapak Zainal Anwari dan pintu surgaku ibu Riskiyah. Terimakasih atas setiap tetes keringat dalam setiap langkah pengorbanan dan kerja keras yang dilakukan untuk memberikan yang terbaik kepada penulis, mengusahakan segala kebutuhan penulis, mendidik, membimbing dan selalu memberikan kasih sayang yang tulus, motivasi, serta dukungan dan mendoakan penulis dalam keadaan apapun agar penulis mampu bertahan untuk melangkah setapak demi setapak dalam meraih mimpi di masa depan. Terimakasih untuk selalu berada di sisi penulis dalam meyelesaikan penulisan skripsi ini hingga memperoleh gelar Sarjana Hukum.
2. Kepada kakak kandung saya khoiril Mahmud dan kakak ipar saya Husnul Khotimah terimakasih banyak atas dukungannya secara moril maupun materil, terimakasih juga atas segala motivasi dan dukungannya yang diberikan kepada penulis mampu menyelesaikan studinya sampai sarjana.
3. Terimakasih juga kepada Keluarga besar saya yang selalu memberikan dukungan, semangat dan doa kepada saya sehingga skripsi ini bisa terselesaikan. Oleh karena itu proses saya selama ini akan dipersembahkan bagi semua orang yang berharga di dalam hidup saya terlebih khususnya keluarga.

KATA PENGANTAR

Alhamdulillah saya sangat bersyukur kepada Allah SWT yang memiliki segalanya yang telah mengasihi kehidupan serta nikmat. Segala nikmat yang begitu mulia dan berangsur-angsur karunianya skripsi sederhana ini akhirnya bias dilewati dengan sukses serta dapat rampung sebagaimana mestinya dengan baik serta lancer sebagai tugas akhir bagi peneliti dalam menempuh pendidikan S1 dimana hal tersebut yang bias mengantar peneliti untuk kejenjang kelulusan serta dengan perjuangan ini peneliti bias mendapatkan gelar Sarjana dengan bangga. Penelitian ini bisa terselesaikan karena adanya suatu dukungan, dan dengan peran dari banyaknya pihak yang ikut serta terlibat dalam penulisannya. Oleh karena itu melalui kata pengantar ini penulis menyampaikan rasa terima kasih yang sedalam-dalamnya kepada:

1. Bapak Rektor Prof. Dr. H. Hepni, S.Ag, M. M. CPEM selaku Rektor UIN Kiai Haji Achmad Siddiq Jember, atas kesempatan dan dukungan fasilitas akademik dalam penulisan skripsi ini.
2. Bapak Dr. Wildani Hefni, M.A. selaku Dekan Fakultas Syariah UN Kiai Haji Achmad Siddiq Jember, yang telah memberikan izin untuk penulisan skripsi ini.
3. Ibu Dr. Hj. Busriyanti. M.Ag., Selaku Wakil Dekan I Fakultas Syariah Universitas islam Negeri Kiai Haji Achmad Siddiq Jember atas dukungan dan perhatian terhadap mahasiswa sangat berarti bagi kami.
4. Bapak Freddy Hidayat, M.H. selaku Koordinator Program Studi Hukum Ekonomi Syariah, yang memberikan bantuan dalam kelancaran proses

penyelsaian skripsi saya.

5. Bapak Dr. H. Martoyo, S.H.I., M.H. selaku Dosen Pembimbing Skripsi, saya ucapkan banyak terima kasih atas bantuan, waktu, arahan, serta bimbingan dan nasihat yang sangat berharga selama proses pengerjaan skripsi ini.
6. Bapak Prof. Dr. H. Miftah Arifin, M.Ag. Selaku Dosen Pembimbing Akademik (DPA) saya di Fakultas Syariah Universitas Islam Negeri Kiai Achmad Siddiq Jember, yang telah mendukung kelancaran prosedur dari awal hingga kelulusan ini.
7. Bapak dan Ibu Dosen Fakultas Syariah UIN Kiai Haji Achmad Siddiq Jember, terima kasih atas ilmu dan pengalaman berharga yang telah diberikan kepada saya selama menjalani masa perkuliahan.
8. Terima kasih kepada seluruh penulis buku/referensi yang telah saya gunakan untuk menyusun skripsi ini.

Jember, 9 Oktober 2025

Penulis

ABSTRAK

Sofia widiatul hasana, **2025**: *Perlindungan Hukum Terhadap Nasabah Korban Phishing Dalam Sistem E-banking di Indonesia*

Kata Kunci: Perlindungan Hukum, Nasabah, *Phishing*, *E-banking*

Perkembangan teknologi informasi mendorong kemudahan transaksi keuangan melalui layanan electronic banking (*e-banking*). Namun juga membawa ancaman kejahatan *phishing* yang mencuri data pribadi dan mengakibatkan kerugian finansial. Perlindungan terhadap keamanan data dan privasi dijamin dalam Pasal 28G ayat (1) UUD 1945 Republik Indonesia, Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan data Pribadi, dan Undang-Undang Nomor 10 tahun 1998 tentang perbankan. Namun, dalam kenyataannya, perlindungan hukum ini belum dilaksanakan secara maksimal karena masih banyak nasabah yang menjadi korban pencurian data dan melalui sistem *e-banking*.

Penelitian ini berfokus pada: 1) Bagaimana bentuk *phishing* dalam aplikasi *e-banking* di Indonesia, 2) Bagaimana akibat *phishing* terhadap nasabah pengguna layanan *e-banking*, 3) Bagaimana perlindungan hukum nasabah terhadap *phishing* dalam sistem *e-banking* di Indonesia.

Tujuan penelitian ini yakni Untuk mengetahui dan menganalisis bentuk *phishing* dalam aplikasi *e-banking* di Indonesia serta Untuk mengetahui dan menganalisis akibat *phishing* terhadap nasabah pengguna layanan *e-banking* dan Untuk mengetahui dan menganalisis perlindungan hukum nasabah terhadap *phishing* dalam sistem *e-banking* di Indonesia?

Penelitian ini menggunakan metode penelitian normatif dengan pendekatan yang digunakan adalah pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus. Dengan menggunakan sumber bahan hukum primer dan sekunder. Analisis bahan hukum yang digunakan berupa penyusunan bahan hukum, klarifikasi bahan hukum, pengelolahan bahan hukum, interpretasi hasil dari pengolahan.

Kesimpulan dari penelitian ini yaitu: 1) *Phishing* merupakan tindak kejahatan siber yang berbentuk penipuan digital untuk mencuri data pelanggan, yang melanggar Pasal 378 Kitab Undang-Undang Hukum Pidana, Undang-Undang ITE, serta Undang-Undang PDP. Pengawasan dilakukan oleh OJK berdasarkan POJK No. 38 tahun 2016. 2) kejahatan ini menyebabkan kerugian finansial, penurunan kepercayaan, dan dampak psikologis, sehingga bank perlu menjaga keamanan dan memberikan perlindungan sesuai dengan Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Konsumen, serta Undang-Undang Perbankan. 3) Perlindungan hukum dilakukan secara preventif dan represif melalui peningkatan keamanan, pendidikan, dan penegakan hukum. Kerjasama antara pemerintah, OJK, dan bank diperlukan untuk memperkuat keamanan siber dan menjaga kepercayaan masyarakat.

DAFTAR ISI

BAB I

PENDAHULUAN

A. Konteks Penelitian

Dengan berjalannya waktu, manusia semakin bertambah kebutuhan dan keinginan sejalan dengan perkembangan zaman. Manusia cenderung mengharapkan segala sesuatu dapat diperoleh dengan mudah selama proses pemenuhan kebutuhan tersebut. Salah satu diantaranya adalah kemajuan teknologi internet, yang telah sangat membantu modernisasi kehidupan masyarakat di banyak bidang, seperti pendidikan, militer, ekonomi, administrasi perbankan, dan sosial. Sebagian besar orang di Indonesia dan banyak di negara lain secara teratur menggunakan uang digital dan melakukan transaksi melalui internet selama era perkembangan teknologi informasi. Karena dianggap sebagai metode yang efisien, fenomena ini dianggap memiliki peran yang signifikan dalam mempercepat pertumbuhan suatu negara.[1]

Masyrakat kini merasakan berbagai keuntungan berkat pesatnya perkembangan teknologi internet. Hal ini menumbuhkan keyakinan bahwa kemajuan teknologi mampu mempermudah aktivitas sehari-hari, terutama dalam hal keuangan. Sebagai dampaknya, layanan berbasis *online* telah merambah ke berbagai bidang bisnis, khususnya sektor perbankan. Saat ini, kemajuan internet sangat membantu industri perbankan dalam meningkatkan kinerja bisnisnya. Nasabah pun dapat melakukan beragam transaksi keuangan

[1]Pangestu, R., & Mardijono, H. A, Upaya Perlindungan Hukum Bagi Korban Penipuan Credit Point Call Of Duty Mobile, (Universitas 17 Agustus 1945, 2023) https://jurnal.untag-sby.ac.id/index.php/sosialita/article/view/8643

secara cepat melalui internet, termasuk melalui sistem *electronic banking (e-banking). E-banking* adalah layanan perbankan yang menggunakan media elektronik untuk melakukan transaksi dan memperoleh informasi.[2] Layanan ini mencakup berbagai fitur seperti ATM, internet *banking*, *mobile banking*, dan SMS *banking.*

Keberadaan *e-banking* memberikan berbagai keuntungan bagi nasabah dan bank, tetapi juga membawa risiko serta dampak negatif. Salah satu kelemahan utama *e-banking* adalah potensi terjadinya kejahatan perbankan, seperti pencurian data pribadi nasabah. Penyalahgunaan data pribadi menjadi masalah yang semakin mendesak di era digital ini, di mana data pribadi sering kali disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Negara memiliki kewajiban konstitusional untuk melindungi semua warga negara, sebagaimana tercantum dalam Pembukaan, Alinea Keempat, Undang-Undang Dasar Republik Indonesia Tahun 1945. Salah satu hak konstitusi yang diatur dalam UUD 1945 adalah hak atas perlindungan pribadi, yang dijelaskan dalam Pasal 28G Ayat (1). Hak pribadi ini mencakup perlindungan terhadap data pribadi dan identitas seseorang. Perlindungan data pribadi sangat penting untuk menjaga kebebasan individu dan mencegah pelanggaran informasi. Oleh karena itu, keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan langkah penting dalam menyediakan perlindungan hukum di era digital. Undang-undang ini bertujuan untuk memberikan perlindungan hukum yang kuat bagi individu terkait

[2] Vanya Agatha Hendarto dan Endang Prasetyawati, "Tanggung Jawab Bank Dalam Mengantisipasi Dan Menangani Kerugian Nasabah Akibat Scam Melalui Link Phising Pada Mobile Banking," *IURIS STUDIA: Jurnal Kajian Hukum* 5, no. 3 (Oktober 2024–Januari 2025), 2.

pengumpulan, penggunaan, dan penyebaran data pribadi mereka, termasuk dalam layanan perbankan digital seperti *e-banking*.[3]

Salah satu perlindungan hukum penting bagi bank adalah menjaga kerahasiaan data, sebagaimana telah diatur dalam beberapa pasal di Undang-Undang No. 10 Tahun 1998 tentang Perubahan atas UU No.7 Tahun 1992 tentang perbankan. Pasal 40 secara khusus menegaskan pentingnya privasi data pelanggan, yang mencakup lebih dari sekedar informasi keuangan. Di sisi lain, nasabah juga diharapkan untuk menjaga kerahasiaan dengan melindungi data pribadi mereka, termasuk nomor telepon. Hal ini menunjukkan tamggung jawab terhadap prinsip kerahasiaan sebagai upaya untuk minimalkan risiko kejahatan perbankan dalam lingkungan e-bangking.[4]

Perkembangan teknologi informasi telah mengubah cara pandang tentang batas wilayah, waktu, nilai-nilai, bentuk objek, pemikiran logis, pola kerja, dan perilaku sosial, beralih dari cara manual menjadi digital. Pengaruh ini telah merubah bentuk, metode, sasaran, dan dampak dari kejahatan berbasis teknologi. Pergeseran paradigma ini, pada kenyataannya, membuat hukum semakin sulit untuk beradaptasi sebagai sarana pengatur sosial. Hukum berfungsi untuk melindungi kepentingan manusia. Untuk melindungi kepentingan ini, hukum perlu diterapkan. Oleh karena itu, perlindungan hukum adalah perlindungan yang diberikan oleh undang-undang untuk

[3]. Dewi Fortuna Mamonto, "Analisis Perlindungan Hukum terhadap Penyalahgunaan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *Jurnal Ilmiah Hukum*, Vol. X, No. X (2022): 5.

[4] Ramadhanti Achlina Tri Putri dan Heru Sugiyono, "Tanggung Jawab Bank Terhadap Tindakan Phising Dalam Sistem Penggunaan E-Banking (Studi: Kasus Phising Pada PT. Bank Rakyat Indonesia (Persero) TBK)," *Jurnal Interpretasi Hukum* 4, no. 3 (Desember 2023).

menjaga kepentingan manusia agar kehidupan dapat berjalan dengan normal, aman, dan tenteram.[5]

Penegakan hukum merupakan kebutuhan penting untuk mencapai keamanan, keadilan, dan manfaat hukum dalam penerapan hukum terhadap kasus-kasus kejahatan di bidang teknologi informasi. Hal ini karena dapat menjadi masalah serius yang mengganggu, yaitu kejahatan yang terjadi di dunia maya atau yang biasa dikenal sebagai kejahatan siber. Kejahatan ini dapat terjadi akibat kelalaian atau kurangnya perhatian dari pengguna komputer dalam melindungi data pribadi dan sensitif mereka, terutama yang berkaitan dengan transaksi keuangan melalui layanan seperti perbankan *online*, dompet elektronik, *e-commerce*, dan *platform* pembayaran. Pesatnya pertumbuhan kejahatan siber menjadi tantangan besar dalam menyesuaikan sistem hukum yang sudah ada. Hukum dituntut untuk dapat melindungi hak-hak korban, menangkap pelaku kejahatan, serta mencegah kasus serupa terjadi dimasa mendatang.[6]

Cybercrime sendiri memiliki banyak macam, salah satunya adalah *phishing*. *Phishing* adalah penipuan elektronik yang dilakukan melalui email palsu, tautan, situs web, pesan teks, atau telepon yang terlihat seperti situs resmi dari unit atau organisasi yang dapat dipercaya, dengan tujuan untuk mendapatkan keuntungan pribadi dengan mengorbankan pelanggan. Pelaku

[5]. Dian Ekawati, "Perlindungan Hukum terhadap Nasabah Bank yang Dirugikan Akibat Kejahatan Skimming Ditinjau dari Perspektif Teknologi Informasi dan Perbankan," *Jurnal Hukum*, Vol. 1, No. 2 (Desember 2018): 157.

[6] Abdul Halim Barkatullah, *Hukum Kejahatan Siber: Tinjauan atas Cyber Crime dan Digital Evidence*, (Yogyakarta: Pustaka Pelajar, 2023), 4-5.

phishing berusaha untuk memperoleh informasi rahasia seperti data pribadi (nama, usia, alamat), informasi akun (nama pengguna, kata sandi), dan data keuangan (informasi kartu kredit, nomor rekening). Serangan *phising* ini merupakan aktivitas kriminal yang terus berkembang dalam dunia perbankan dan memanfaatkan teknik rekayasa sosial yang membuat korban tertipu dan rela memasukkan data pribadi mereka ke dalam situs palsu yang dibuat menyerupai situs asli, yang akhirnya menyebabkan kerugian bagi korban.[7]

Phishing merupakan salah satu jenis kejahatan siber yang semakin meningkat, terutama dalam sektor perbankan. Pada dasarnya, *phishing* adalah tindakan kriminal di mana pelaku berpura-pura menjadi individu atau entitas tepercaya melalui pesan elektronik untuk mendapatkan informasi pribadi dan rahasia dari korban. Metode ini umumnya berkaitan dengan cara-cara rekayasa sosial. Undang-Undang Nomor 19 Tahun 2016, yang mengubah Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik, menyatakan bahwa setiap orang dilarang secara sengaja dan tanpa wewenang, atau secara ilegal, mengakses komputer dan/atau sistem elektronik dalam bentuk apa pun yang mencakup pelanggaran, penembusan, pengabaian, atau peretasan terhadap sistem keamanan.[8]

Perlindungan hukum sangat berkaitan dengan meningkatnya kepercayaan dan rasa aman yang dirasakan oleh pelanggan dalam sebuah sistem, oleh karena itu, perlindungan hukum yang memadai sangat penting.

[7]. Mayline Djuminar Silitonga, "Perlindungan Hukum Atas Kerugian Nasabah Bank Akibat Modus *Phishing*" (Skripsi, Universitas HKBP Nommensen, 2023), 2-3.

[8] Akhmad Fery Hasanudin, A Basuki Babussalam, "Upaya Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking" *Gagasan Hukum*, Vol. 6, no. 01 (2024):

Namun, lebih dari sekadar kemudahan dari fasilitas yang ditawarkan oleh *e-banking*, dari presektif hukum, keberadaan layanan *e-banking* ini masih dihadapkan pada permasalahan kejahatan *phishing* yang belum terselesaikan. Kondisi ini menjadi semakin parah dan kompleks akibat dari perubahan fasilitas *e-banking* yang sangat cepat, baik dari sisi teknologi yang digunakan maupun dari perkembangan aktivitas bisnisnya. Berdasarkan kenyataan dan realitas yang telah disebutkan sebelumnya, kini muncul kebutuhan yang mendesak untuk mengembangkan ide-ide baru mengenai betapa pentingnya makna hukum dalam mengatur berbagai isu dan persolan yang muncul dalam layanan *e-banking*.[9]

Ancaman *phishing* semakin merajalela, pada kuartal 2023 kasus *phishing* di indonesia mencapai 26.675 kasus, seperti kasus pada tahun 2023, tepatnya dibulan juli. Dalam sebuah kasus di Surabaya, seorang nasabah kehilangan Rp 1,4 miliar karena penipuan daring. Korban melaporkan kejadian tersebut ke Kepolisian Daerah Jawa Timur. Penyelidikan menunjukkan bahwa pada akhir Mei 2023, korban menerima undangan pernikahan digital. Setelah mengeklik undangan tersebut di ponselnya, ia menerima notifikasi iklan dan merasa ada yang tidak beres. Ia kemudian memeriksa saldo rekening tabungannya melalui *e-banking*, hanya untuk menemukan bahwa Rp 1,4 miliar yang awalnya ada telah hilang. hingga hanya tersisa 2 juta pada saldo *e-banking*.[10] Kejadian ini menegaskan bahwa

[9] Intan Selviany, "Efektifittas Pelaksanaan Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan Terhadap Pengguna Teknologi Informasi Internet Banking" *(*Skripsi, Universitas Putera Batam, 2019), 11.

[10] https://www.berisatu.com. Di akses pada 1 Agustus 2025.

kejahatan *phishing* memanfaatkan kelemahan kesadaran keamanan digital masyarakat dan teknik rekayasa yang meyakinkan.

Contoh kasus *phishing* lainnya yang telah sampai hingga pengadilan yaitu sebagaimana dalam tiga putusan berikut: Pertama, Putusan Nomor 958/Pid. Sus/2020/PNPbr. Dalam kasus ini, hakim memutuskan untuk menjatuhkan hukuman kepada Terdakwa berupa penjara selama 1 tahun dan 2 bulan serta denda sebesar Rp 20. 000. 000,-. Jika Terdakwa tidak membayar denda tersebut, maka akan mengalami hukuman penjara selama 1 bulan sebagai gantinya. Kedua, Putusan Nomor 73/Pid. Sus/2021/PN Nga, di mana hakim memutuskan menjatuhkan hukuman penjara selama 3 tahun kepada Terdakwa serta denda sebesar Rp 100. 000. 000,00. Jika denda itu tidak dibayar, Terdakwa akan mendapatkan hukuman penjara selama 3 bulan. Ketiga, Putusan Nomor 845/Pid. Sus/2020/PT Sby, hakim menjatuhkan hukuman penjara selama 8 bulan kepada Terdakwa. Mengingat ringan nya sanksi bagi pelaku phising, ajukan banding dengan tuntutan hukuman 2 tahun penjara dan denda sebesar Rp 30. 000. 000, jika denda tersebut tidak dibayar maka akan diganti dengan penjara selama 2 bulan.[11]

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk memahami bentuk-bentuk kejahatan *phishing* dalam aplikasi *e-banking* di Indonesia, menganalisis dampak yang ditimbulkan terhadap nasabah, serta menilai bagaimana perlindungan hukum diberikan kepada korban. Penelitian ini diharapkan dapat membantu meningkatkan keamanan digital dan

[11] Mirza Dhafa Izzulahaq, *Perlindungan Hukum Terhadap Korban Phising Yang Terjadi Di Indonesia*, Skripsi, Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Negeri Semarang, 2024, 4.

perlindungan hukum di sektor perbankan.

B. Fokus Penelitian

1. Bagaimana bentuk *phishing* dalam aplikasi *e-banking* di Indonesia?
2. Bagaimana akibat *phishing* terhadap nasabah pengguna layanan *e-banking?*
3. Bagaimana perlindungan hukum nasabah terhadap *phishing* dalam sistem *e-banking* di Indonesia?

C. Tujuan Penelitian

1. Untuk mengetahui dan menganalisis bentuk *phishing* dalam aplikasi *e-banking* di Indonesia?
2. Untuk mengetahui dan menganalisis akibat *phishing* terhadap nasabah pengguna layanan *e-banking*?
3. Untuk mengetahui dan menganalisis perlindungan hukum nasabah terhadap kejahatan *phishing* dalam sistem *e-banking* di Indonesia?

D. Manfaat Penelitian

Adapun dengan terlaksananya tujuan penelitian di harapkan bisa memberikan Kemanfaatan sebagaimana terdapat 2 manfaat yaitu teoritis dan praktis

1. Manfaat Teoritis
   a. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan ilmu hukum, khususnya di bidang hukum perbankan dan hukum kejahatan *phishing*.
   b. Hasil penelitian ini dapat menjadi bahan tambahan literatur yang

membahas mengenai perlindungan hukum terhadap nasabah korban kejahatan *phishing* dalam sistem *e-banking*.

2. Manfaat Praktis

   a. Bagi Lembaga Perbankan, sebagai bahan evaluasi dalam memperkuat sistem keamanan informasi dan meningkatkan upaya pencegahan kejahatan *phishing* terhadap nasabah.

   b. Bagi Pemerintah dan Pembuat Kebijakan, sebagai bahan pertimbangan untuk menyusun atau menyempurnakan peraturan perundang-undangan yang relavan dengan perlindungan konsumen dalam transaksi digital.

   c. Bagi Otoritas Jasa Keungan (OJK), penelitian ini dapat menilai dan memperbaiki peraturan mengenai penerapan manajemen risiko teknologi informasi disektor perbankan, memperkuat pengawasan terhadap pelaksanaan standar keamanan siber, meningkatkan literasi keuangan digital masyarakat untuk mencegah phising, serta mendorong kerjasama antara OJK, penegak hukum, dan institusi perbankan dalam menangani kasus *phishing*.

   d. Bagi Nasabah, penelitian ini diharapkan dapat meningkatkan kesadaran dan pengetahuan tentang risiko *phishing*, serta mendorong masyarakat agar lebih berhati-hati dalam menjaga kerahasiaan data pribadi saat menggunakan layanan *e-banking*.

E. Definisi Istilah

Berikut merupakan beberapa istilah yang tercantum dalam judul proposal ini, diantaranya:

a. Perlindungan Hukum

Kamus Besar Bahasa Indonesia (KBBI) mendefinisikan "Perlindungan" sebagai sesuatu atau tindakan yang memberikan perlindungan.[12] Kemudian, "Hukum" diartikan sebagai suatu peraturan atau kebiasaan yang secara resmi dianggap mengikat, yang ditegaskan oleh pemimpin atau pemerintah.[13] Perlindungan hukum adalah semua usaha yang dilakukan negara melalui instrumen hukum untuk menjamin, melindungi, dan menegakkan hak-hak warga negara dari berbagai bentuk pelanggaran, baik oleh individu, kelompok, maupun lembaga..[14]

b. Nasabah

Seorang nasabah adalah istilah untuk seseorang yang memanfaatkan layanan dan fasilitas keuangan dalam dunia perbankan dan keuangan. Istilah "pelanggan" sering digunakan untuk merujuk pada individu atau entitas hukum yang menjadi nasabah sebuah lembaga keuangan.[15] Berdasarkan Undang-Undang No. 10 tahun 1998, pelanggan merupakan pihak yang memanfaatkan layanan bank, baik sebagai penyimpan dana maupun sebagai penerima fasilitas kredit atau

[12] Kamus Besar Indonesia (online, di akses 1 Agustus 2025) https:kbbi.web.id/perlindungan

[13] Kamus Besar Indonesia (online, di akses 1 Agustus 2025) https:kbbi.web.id/hukum

[14] Philipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat di Indonesia: Sebuah Studi tentang Prinsip-prinsipnya, Penanganannya oleh Peradilan dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi Negara* (Surabaya: Bina Ilmu, 1987), 25.

[15] https://www.megasyariah.co.id. Diakses ada tanggal 1 agustus 2025

pembiayaan berdasarkan perjanjian dengan bank.[16]

c. *Phishing*

Phishing adalah upaya penipuan untuk memperoleh informasi pribadi, data akun atau data finansial korban melalui email, pesan teks, atau platfrom *online*, dengan tujuan memanfaatkan data tersebut untuk kejahatan.[17] Dalam kamus hukum, *phishing* didefinisikan sebagai upaya memperoleh data sensitif dengan menyamar sebagai entitas terpercaya.[18] Menurut Brian Krebs, *phishing* merupakan teknik rekayasa sosial yang mengecoh korban agar sukarela menyerahkan data pribadinya.[19] Di Indonesia, *phishing* termasuk tindak pidana berdasarkan UU ITE (Pasal 30 & 35)[20] dan pelanggaran perlindungan data menurut UU PDP yang dapat dikenai sanksi pidana dan administratif.[21]

d. *E-banking (Electronic Banking)*

E-banking menurut Kamus Besar Bahasa Indonesia (KBBI) ialah layanan perbankan dan produk perbankan secara langsung kepada pelanggan melalui elekronik, saluran komunikasi interaksi.[22] *E-banking* adalah layanan yang disediakan oleh perbankan untuk menjalankan aktivitas perbankan melalui saluran elektronik, terutama internet, dengan

[16] Sekretariat Negara Republik Indonesia, Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, Pasal 1.

[17] DJPB Kemenkeu, *Phishing:Pengertian, Jenis, dan Cara Menghindari Phishing, 2025*, https://djppb.kemenkeu.go.id.

[18] Lili Rasjidi dan I.B. Wyasa Putra, *Kamus Hukum: Bahasa Indonesia–Bahasa Inggris* (Bandung: Citra Aditya Bakti, 2015), 162.

[19] Brian Krebs, *Spam Nation* (Sourcebooks, 2014), 47.

[20] UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Pasal 30 & 35.

[21] UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, Bab V.

[22] Kamus Besar Bahasa Indonesia (online, diakses 1 agustus 2025) https://kbbi.web.id/e-banking

memanfaatkan teknologi informasi dan komunikasi untuk menghemat waktu dan biaya bagi pihak bank maupun nasabah.[23]

Berdasarkan definisi istilah yang sudah dipaparkan diatas, Perlindungan hukum terhadap nasabah korban kejahatan *phishing* dalam sistem *e-banking* di Indonesia adalah upaya hukum untuk memastikan, melindungi, dan menegakkan hak-hak nasabah yang dirugikan oleh tindakan kejahatan *phishing* dalam dunia perbankan digital. Upaya perlindungan ini didasari oleh undang-undang yang mengatur tentang keamanan data pribadi serta kewajiban lembaga keuangan dalam menjaga kerahasiaan informasi nasabah. *Phishing* adalah pada kejahatan yang meniru entitas resmi untuk mendapatkan informasi pribadi atau keuangan korban melalui media elektronik. Sedangkan *e-banking* adalah layanan perbankan yang berbasis teknologi informasi yang memudahkan proses transaksi keuangan. Oleh karena itu, perlindungan hukum ini bertujuan untuk memberikan kepastian hukum, rasa aman, dan keadilan bagi nasabah pengguna layanan *e-banking* di Indonesia.

F. Sistematika Pembahasan

Sistematika pembahasan merupakan suatu rancangan yang nantinya akan digunakan untuk menyejikan dan mengorganisir suatu pembahasan atau penulisan dengan tujuan untuk mempermudah pemahaman pembaca atau pendengar dan memberikan alur logistic dalam menyampaikan informasi. Umumnya sistematika pembahasan terdiri dari beberapa bagian yang secara

[23] Aditya Wardhana, *Pemanfaatan Teknologi Digital dalam Berbagai Aspek Kehidupan Masyarakat* (Bandung: CV Media Sains Indonesia, 2021), 81.

sistematis menguraikan topik atau masalah yang dibahas. Maka sistematika pembahasan pada penelitian yang dibuat dalam skripsi ini adalah:

BAB I PENDAHULUAN

Dalam pendahuluan ini merupakan bagian awal yang akan mendiskripsikan Gambaran umum terkait topik atau masalah yang akan dibahas, dan didalam pendahuluan ini terdapat beberapa komponen didalamnya yakni, konteks penelitian, tujuan penelitian, manfaat penelitian, definisi istilah dan sistematika pembahasan.

BAB II TINJAUAN PUSTAKA

Pada bagian ini berisi uraian mengenai kajian pustaka yang mana terdapat penelitian terdahulu serta kajian teori yang mempunyai keterkaitan dengan pembahasan yang akan diteliti yakni Perlindunga Hukum Terhadap Nasabah Korban Kejahatan Phising Dalam Sistem *E-banking* Di Indonesia. Adapun tujuan memaparkan penelitian terdahulu sebagai penguat dan perbedaan dari penelitian yang akan peneliti lakukan agar terdapat kemenarikan tersendiri dari penelitian lainnya, ataupun dalam kajian teori yaitu sebuah gambaran umum yang relavan dengan judul penelitian.

BAB III METODE PENELITIAN

Bagian ini menjelaskan metode penelitian yang akan digunakan oleh peneliti untuk menjawab pertanyaan penelitian. Ini mencakup jenis penelitian, pendekatan penelitian, sumber data, teknik pengumpulan data hukum, validitas data hukum, dan tahapan penelitian.

BAB IV PEMBAHASAN

Bab ini membahas ide penelitian dan penyampaian hasil akhir penelitian. Bab ini menggambarkan fokus masalah yang telah ditentukan sebelumnya. Bagian ini menjelaskan pemikiran dan analisis peneliti terhadap masalah tersebut.

BAB V PENUTUP

Kesimpulan terdiri dari dua sub-bab: yang pertama membahas kesimpulan dari pemaparan data dan analisis hasil penelitian, dan yang kedua menguraikan saran dan rekomendasi untuk tindak lanjut penelitian yang telah dilakukan.

BAB II

KAJIAN PUSTAKA

A. Peneliti Terdahulu

Sebagai salah satu pembuktian bahwasannya penelitian ini bersifat asli, maka peneliti melakukan berbagai kajian dari peneliti-peneliti terdahulu sebagai bahan perbandingan yang ditinjau dari sisi kesamaan dan perbedaan penelitian yang akan dilakukan. Berikut merupakan kajian-kajian yang peneliti temukan dari beberapa peneliti-peneliti terdahulu.

1. Perlindungan Hukum Bank Terhadap Nasabah Korban Modus *Phishing* WhatsAppp Melalui PDF Palsu Studi Kajian Berdasarkan UU No 10 Tahun 1998 Tentang Perbankan dan Kompilasi Hukum Ekonomi Syariah[25]

   Skripsi yang ditulis oleh Mela Intan Yesica Mahasiswi Program Studi Hukum konomi Syariah Universitas Islam Negeri Maulana Malik Ibrahim Malang ini membahas mengenai bentuk perlindungan hukum yang diberikan oleh bank kepada nasabah yang menjadi korban modus *phishing* melalui PDF palsu di alplikasi *WhatsApp*.

   Fokus permasalahan pada skripsi ini yaitu: *pertama,* bagaimana bank memberikan perlindungan hukum terhadap nasabahnya yang menjadi korban modus *phishing WhatsApp*? *Kedua,* bagaimana keterkaitan perlindungan hukum nasabah korban modus *phishing* WhatsApp melalui PDF palsu perspektif hukum ekonomi syariah?

[25] Mela Intan Yesica, "Perlindungan Hukum Bank Terhadap Nasabah Korban Modus *Phishing* WhatsAppp Melalui PDF Palsu Studi Kajian Berdasarkan UU No 10 Tahun 1998 Tentang Perbankan dan Kompilasi Hukum Ekonomi Syariah". (Skripsi, Universitas Islam Negeri Maulana Malik Ibrahim Malang, 2024)

Penelitian ini menggunakan pendekatan yuridis normatif, dengan menganalisis data sekunder berupa bahan hukum dan literatur terkait. Data-data ini kemudian dianalisis secara komprehensif untuk memahami perlindungan hukum yang diberikan oleh bank kepada nasabah korban phising *WhatsApp*, serta untuk mengevaluasi konsistensi dengan Undang-Undang Perbankan dan Kompilasi Hukum Ekonomi Syariah.

Hasil penelitian menunjukkan bahwa bank memiliki tanggung jawab hukum untuk melindungi nasabahnya dari ancaman kejahatan siber, termasuk modus phising *WhatsApp*. Perlindungan tersebut harus memperhatikan ketentuan yang ada dalam UU No 10 tahun 1998 dan prinsip-prinsip hukum ekonomi syariah seperti amanah, kejujuran, dan tanggung jawab. Meskipun demikian, masih diperlukan upaya lebih lanjut untuk memperkuat perlindungan hukum tersebut agar lebih efektif dalam menghadapi tantangan kejahatan siber di masa depan dan memperjelas perlindungan hukum terhadap nasabah.

Persamaan penelitian tersebut dengan penelitian yang dilakukan penulis terletak pada pembahasan mengenai kejahatan *phishing* yang menimpa nasabah bank, serta bentuk perlindungan hukum yang diberikan kepada para korban. Perbadaannya ialah skripsi yang disusun oleh Mela Intan Yesica secara khusus membahas mengenai *phishing* yang terjadi melalui aplikasi WhatsApp dengan modus file PDF palsu dan di analisis menggunakan perspektif hukum ekonomi syariah. Sedangkan penelitian penulis mencakup permasalahan *phishing* dalam layanan e banking secara

umum.

2. Pengaruh Ancaman *Phishing*, Kepercayaan Nasabah dan Keamanan Nasabah Pada Pengguna Mobile Banking di PT.BRI (PERSERO) TbkKantor Cabang Jember[26]

Skripsi yang ditulis oleh Lilis Wahyuningsi Mahasiswi Program Studi Ekonomi dan Bisnis Islam Universitas Islam Negeri Kiai Haji Achmad Siddiq Jember ini membahas mengenai ancaman *phishing* dalam layanan perbankan *online* terjadi akibat kombinasi antara teknik manipulasi sosial oleh pelaku dan kerentanan pengguna.

Skripsi ini membahas empat poin penting: pertama, apakah ancaman *phishing* berpengaruh terhadap pengguna mobile banking di Bank BRI Cabang Jember? kedua, apakah kepercayaan nasabah mempengaruhi pengguna mobile banking di Bank BRI Cabang Jember? ketiga, apakah keamanan nasabah berdampak pada pengguna mobile banking di Bank BRI Cabang Jember? keempat, bagaimana ancaman *phishing*, kepercayaan nasabah, dan keamanan nasabah memengaruhi pengguna mobile banking di Bank BRI Cabang Jember?

Metode yang digunakan dalam penelitian ini adalah pendekatan kuantitatif. Populasi umum dalam studi ini mencakup seluruh nasabah Bank BRI Cabang Jember dari bulan Januari 2023 hingga Desember 2023, yang jumlahnya mencapai 7. 358 nasabah. Penelitian ini bersifat

[26] Lilis Wahyuningsi, "Pengaruh Ancaman *Phishing*, Kepercayaan Nasabah dan Keamanan Nasabah Pada Pengguna Mobile Banking di PT.BRI (PERSERO) Tbk Kantor Cabang Jember*"* (Skripsi, Universitas Islam Negeri Kiai Haji Achmad Siddiq Jember,2024)

kuantitatif, dan metode pengambilan sampel yang digunakan adalah simple random sampling, di mana sampel diambil secara acak tanpa mempertimbangkan strata. Sebanyak 100 nasabah diambil sebagai sampel. Pengolahan data dilakukan dengan menggunakan SPSS versi 27. 0.

Hasil penelitian menunjukkan bahwa secara parsial, ancaman *phishing* memberikan dampak yang signifikan terhadap pengguna mobile banking di BRI (BRIMO), kepercayaan pelanggan memberikan pengaruh yang signifikan terhadap pengguna mobile banking di BRI (BRIMO), dan keamanan pelanggan juga memberikan dampak yang signifikan terhadap pengguna mobile banking di BRI (BRIMO). Secara bersamaan, ancaman *phishing*, kepercayaan pelanggan, dan keamanan pelanggan memiliki dampak yang signifikan terhadap pengguna mobile banking di BRI (BRIMO).

Persamaan penelitian ini dengan yang akan dilakukan penulis ialah sama sama terletak pada objek kajian yaitu kejahatan *phishing* yang berdampak langsung pada nasabah bank, khususnya dalam konteks digital banking. Sedangkan perbedaannya yaitu penelitian terletak pada cakupan dan arah pembahasannya. Penelitian Lilis bersifat terbatas secara geografis dengan fokus pada studi kasus di BRI Wonokromo, serta mengulas keterlibatan aparat penegak hukum dalam penyelesaian kasus. Sebaliknya, penelitian penulis membahas isu *phishing* dalam sistem *e-banking* secara nasional dan lebih menekankan pada analisis hukum positif, regulasi digital, serta perlindungan data pribadi sebagai bagian dari upaya

melindungi nasabah.

3. Perlindungan Hukum Terhadap Nasabah Bank Syariah Indonesia Dari Serangan Cybercrime[27]

Skripsi yang ditulis oleh Ballqish Amelia Assiffa Mahasiswi Program Studi Hukum Ekonomi Syariah Universitas Islam Negeri Syarif Hidayatullah ini membahas mengenai upaya Bank Syariah Indonesia dalam menghadapi serangan *ransomware***,** serta mengevaluasi sistem perlindungan hukum terhadap nasabah dari sisi kelemahan sistem keamanan internal dan regulasi.

Fokus permasalahan pada penelitian ini yaitu: pertama, Apa Faktor Penyebab Bank Syariah Indonesia Mengalami Serangan Cybercrime? Kedua, Bagaimana Upaya Perlindungan Hukum Bagi Nasabah Terhadap Serangan Cybercrime di Bank Syariah Indonesia?

Penelitian ini menggunakan metode penelitian Normatif Yuridis, dan Analisis data menggunakan Penelitian Kualitatif dan Pendekatan Undang-Undang (statue approach), data yang digunakan berupa data primer yang bersumber dari wawancara dengan pihak yang bersangkutan, kemudian data sekunder yang berasal dari peraturan-peraturan yang berlaku, serta data tersier yang digunakan bersumber dari buku-buku, jurnal, website serta sumber lainnya yang berkaitan dengan penelitian ini.

Hasil dari penelitian tersebut ialah gangguan layanan pada Bank Syariah Indonesia (BSI) disebabkan oleh serangan cybercrime berupa

[27] Ballqish Amelia Assiffa, "Perlindungan Hukum Terhadap Nasabah Bank Syariah Indonesia Dari Serangan Cybercrime". (Skripsi, Universitas Islam Negeri Syarif Hidayatullah, 2023)

ransomware sebagai faktor eksternal, serta kelemahan sistem keamanan internal**,** termasuk kurangnya kompetensi SDM dan kebijakan teknologi yang tidak terintegrasi. Sebagai bentuk perlindungan dan pemulihan, BSI memperkuat sistem keamanan IT serta menerapkan *Business Continuity Plan* (BCP) guna meminimalkan risiko dan kerugian akibat serangan serupa di masa mendatang.

Persamaan penelitian ini dengan yang akan dilakukan penulis ialah sama sama membahas perlindungan hukum terhadap nasabah perbankan digital dari kejahatan siber. Sedangkan perbedaannya adalah Peneliti lebih berfokus pada serangan siber secara menyeluruh, terutama yang berkaitan dengan malware dan gangguan sistem di Bank Syariah Indonesia (BSI). Sedangkan penulis ini lebih spesifik meneliti bentuk kejahatan *phishing*, dan perlindungan hukum nasabah *e-banking* secara spesifik dan menyeluruh.

4. Perlindungan Hukum Terhadap Nasabah atas Kejahatan *Phishing* dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia[28]

Jurnal karya ini ditulis oleh Salsabila Chairunnisa, Tarsisius Murwadji, Nun Harrieti *jurnal hukum dan sosial* 2, no 1 ini membahas bentuk pertanggungjawaban bank digital dan perlindungan hukum atas kejahatan *phishing* dan hacking terhadap nasabah pada layanan bank digital.

[28] Salsabila Chairunnisa, Tarsisius Murwadji, dan Nun Harrieti, "Perlindungan Hukum Terhadap Nasabah atas Kejahatan *Phishing* dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia*" jurnal hukum dan sosial* 2, no 1 (februari 2024)

Fokus permasalahan pada penelitian ini yaitu untuk memahami bagaimana petanggungjawaban bank terhadap nasabah atas kejahatan *phishing* dan hacking ditinjau berdasarkan hukum positif indonesia.

Penelitian ini menggunakan pendekatan hukum normatif. Peneliti melaksanakan studi melalui penelitian perpustakaan, pengumpulan data sekunder yang terdiri dari bahan hukum primer, sekunder, dan tersier, serta studi lapangan yang berhubungan dengan objek penelitian.

Hasil penelitian tersebut bahwa tanggung jawab bank digital mengenai kejahatan *phishing* dan peretasan terhadap pelanggan saat menggunakan layanan bank digital ditelaah berdasarkan Hukum Positif Indonesia, bank digital memiliki kewajiban untuk mengonfirmasi adanya kejahatan *phishing* dan hacking, serta menyediakan layanan aduan yang bisa diakses oleh nasabah selama 24 jam setiap hari. Bank wajib menanggung kerugian yang dialami oleh nasabah guna menjaga kepercayaan nasabah terhadap bank.

Persamaan penelitian tersebut dengan yang dilakukan oleh penulis adalah sama-sama membahas perlindungan hukum nasabah terhadap kejahatan siber disektor perbankan, sama-sama mengacu pada UU ITE, dan UU Perbankan. Sedangkan perbedaannya adalah peneliti mengkaji *phishing* dan hacking pada bank digital sedangkan penulis membahas *phishing* pada layanan *e-banking*.

5. Tanggung Jawab Bank Terhadap Tindakan *Phishing* Dalam Sistem Penggunaan *E-banking* (Studi: Kasus *Phishing* Pada PT. Bank Rakyat Indonesia (Persero) TBK)[29]

Jurnal karya ini ditulis oleh Ramadhanti Achlina Tri Putri, Heru Sugiyono *Jurnal Interpretasi Hukum* 4, no. 3 ini membahas studi perlindungan hukum bagi nasabah bank terkait serangan *phishing* dalam sistem *e-banking* di Indonesia.

Penelitian ini berfokus pada pemahaman bagaimana kerangka hukum di Indonesia melindungi nasabah bank dari risiko *phishing*, khususnya dalam konteks transaksi perbankan digital. Metode penelitian yang digunakan adalah pendekatan normatif yuridis melalui pendekatan undang-undang dan pendekatan kasus.

Hasil dari penelitian tersebut yaitu bahwa Perlindungan hukum terhadap nasabah korban *phishing* dalam *e-banking* dilakukan melalui prinsip kerahasiaan bank, dengan upaya preventif berupa edukasi dan represif melalui penyelesaian sengketa secara hukum. Bank BRI bertanggung jawab dengan menyediakan layanan pengaduan, melakukan penyelidikan, dan membantu nasabah menyelesaikan kerugian. Penelitian ini juga menekankan pentingnya regulasi khusus *e-banking* dan pengawasan lebih optimal dari pemerintah, OJK, dan bank mengingat risiko besar *phishing* terhadap data nasabah dan reputasi bank.

Persamaan penelitian tersebut dengan yang akan dilakukan oleh

[29] Ramadhanti Achlina Tri Putri dan Heru Sugiyono, "Tanggung Jawab Bank Terhadap Tindakan Phising Dalam Sistem Penggunaan E-Banking (Studi: Kasus Phising Pada PT. Bank Rakyat Indonesia (Persero) TBK)" *Jurnal Interpretasi Hukum* 4, no. 3 (Desember 2023).

penulis adalah sama-sama fokus membahas mengenai tindak kejahatan *phishing* dalam sistem *e-banking* serta bentuk tanggung jawab dan perlindungan hukum terhadap nasabah sebagai korban. Sedangkan perbedaannya adalah peneliti menitikberatkan pada studi kasus di PT. Bank Rakyat Indonesia (Persero) Tbk, sedangkan penulis ini memiliki ruang lingkup yang lebih luas dan bersifat normatif, dengan mengkaji perlindungan hukum bagi nasabah korban *phishing* secara menyeluruh berdasarkan ketentuan hukum positif yang berlaku di Indonesia.

Untuk mempermudah dalam pemahaman terkait penelitian terdahulu, maka penulis mencantumkan sebuah tabel. Berikut tabel yang dilampirkan oleh penulis yang memiliki hubungan atau korelasi dengan penelitian yakni sebagai berikut:

Tabel 2.1 Ringkasan Pembahasan dan Perbedaan Penelitian Terdahulu

No.	Nama/Tahun/Judul	Persamaan	Perbedaan
1.	Mela Intan Yesica, 2024, Perlindungan Hukum Bank Terhadap Nasabah Korban Modus *Phishing* WhatsAppp Melalui PDF Palsu.	Persamaan antara penelitian ini dengan penelitian yang penulis angkat ialah sama-sama meneliti tentang kejahahatan *phishing* yang menimpa nasabah.	Perbedaannya adalah skripsi lain membahas mengenai *phishing* melalui WhatsAppp dengan modus file PDF palsu dan di analisis menggunakan prespektif hukum ekonomi syariah. Sedangkan penulis mencakup permasalahan phising dalam layanan *e-banking* secara umum

2.	Lilis Wahyuningsi, 2024, Pengaruh Ancaman *Phishing*, Kepercayaan Nasabah dan Keamanan Nasabah Pada Pengguna Mobile Banking di PT.BRI (PERSERO) Tbk Kantor Cabang Jember	Persamaan penelitian tersebut dengan penelitian yang di lakukan penulis ialah sama sama terletak pada objek kajian yaitu kejahatan *phishing* yang berdampak langsung pada nasabah bank	Perbedaannya ialah yaitu Skripsi lain bersifat terbatas secara geografis dengan fokus ada studi kasus di BRI Wonokromo, sedangkan penelitian penulis membahas isu *phishing* dalam sistem *e-banking* secara umum.
3.	Ballqish Amelia Assifa, 2023, Perlindungan Hukum Terhadap Nasabah Bank Syariah Indonesia Dari Serangan Cybercrime	Persamaan penelitian tersebut dengan penelitian yang di lakukan penulis ialah sama sama membahas perlindungan hukum terhadap nasabah perbankan digital dari kejahatan siber disektor perbankan.	perbedaannya adalah skripsi lain lebih mengkaji *phishing* dan hacking pada bank digital. Sedangkan penulis ini lebih spesifik meneliti bentuk kejahatan *phishing* dalam sistem *e-banking*.
4.	Salsabila Chairunnisa, Tarsisius Murwadji, dan Nun Harrieti, 2024 Perlindungan Hukum Terhadap Nasabah atas Kejahatan *Phishing* dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia.	Persamaan penelitian tersebut dengan penelitian yang di lakukan penulis ialah sama-sama terletak pada fokus pembahasan mengenai perlindungan hukum terhadap nasabah	perbedaannya adalah peneliti membahas beberapa bentuk kejahatan perbankan secara umum dan terbatas pada studi kasus di BSI KC Cibubur sedangkan penulis lebih spesifik membahas kejahatan *phishing* dalam sistem *e-banking*

5.	Ramadhanti Achlina Tri Putri, Heru Sugiyono, 2023, Tanggung jawab Bank Terhadap Tindakan *Phishing* Dalam Sistem Penggunaan *E-banking* (Studi: Kasus *Phishing* Pada PT. Bank Rakyat Indonesia (Persero) TBK)	Persamaan penelitian tersebut dengan penelitian yang di lakukan penulis ialah sama-sama fokus membahas mengenai tindak kejahatan *phishing* dalam sistem *e-banking* serta bentuk tanggung jawab dan perlindungan hukum terhadap nasabah sebagai korban	Perbedaannya perbedaannya adalah peneliti menitikberatkan pada studi kasus di PT. Bank Rakyat Indonesia (Persero) Tbk, sedangkan penelitian ini memiliki ruang lingkup yang lebih luas dan bersifat normatif, dengan mengkaji perlindungan hukum bagi nasabah korban *phishing* secara menyeluruh berdasarkan ketentuan hukum positif yang berlaku di Indonesia

Berdasarkan penjelasan serta pemetaan kajian dari peneliti terdahulu yang memiliki fokus penelitian yang berbeda-beda sesuai dengan penelitian yang diangkat penulis, tidak ada penulis yang membahas subjek yang sama. Adapun hasil penelitian yang memiliki perbedaan dalam isi pembahasan serta objek yang dikaji juga tidak memiliki kesamaan. Oleh karena itu, peneliti mengangkat penelitian yang menganalisis mengenai perlindungan hukum terhadap nasabah korban kejahatan *phishing* dalam sistem *e-banking* di Indonesia.

B. Kajian Konseptual

1. Konsepsi Perlindungan Hukum

a. Pengertian Perlindungan Hukum

Perlindungan hukum terhadap hak asasi manusia dari berbagai bentuk kerugian merupakan salah satu aspek dalam teori perlindungan hukum. Perlindungan hukum merupakan usaha yang dilakukan oleh

petugas penegak hukum untuk memberikan rasa aman, baik secara fisik maupun mental, kepada setiap individu dari berbagai bentuk ancaman atau bahaya.[30]

Soedjono Dirdjosisworo memandang hukum dari delapan perspektif yang berbeda, menunjukkan bahwa hukum itu kompleks dan tidak bisa disederhanakan hanya sebagai undang-undang tertulis atau aparat penegak hukum saja. Perspektif tersebut mencakup hukum sebagai Penguasaan, Petugas, Sikap Tindakan, Tata Hukum, Ilmu Hukum, Disiplin Hukum. Dari berbagai sudut pandang ini, Soedjono Dirdjosisworo menekankan bahwa hukum jauh lebih luas dari sekadar peraturan tertulis dan aparat penegak hukum, yang seringkali menjadi pemahaman umum di masyarakat. Hukum juga mencakup norma-norma yang tumbuh dan berkembang melalui interaksi sosial dalam masyarakat. Masyarakat memiliki beragam kepentingan, dan perbedaan kepentingan ini memerlukan adanya hukum untuk mengatur dan menyeimbangkan berbagai kepentingan tersebut, sehingga tercipta ketertiban dan keadilan.[31]

Menurut Fitzgerald, yang mengutip pendapat Salmond, teori perlindungan hukum menyatakan bahwa hukum berfungsi untuk menyeimbangkan berbagai kepentingan dalam masyarakat. Hukum hadir untuk menentukan prioritas dan batasan karena tidak semua kepentingan bisa dipenuhi sekaligus. Dengan kata lain, hukum adalah

[30] Satjipto Rahardjo, *Ilmu Hukum* (Bandung: Citra Aditya Bakti, 2014), 74
[31] Soedjono Dirdjosisworo, *Pengantar Ilmu Hukum* (Jakarta: Raja Grafindo Persada, 2008), 25-43.

penentu utama kepentingan manusia mana yang harus diatur dan dilindungi.[32]

b. Bentuk Perlindungan hukum

Philipus M. Hadjon mengemukakan bahwa terdapat dua jenis perlindungan hukum yang diberikan pemerintah kepada rakyat, yaitu:[33]

1) Perlindungan hukum preventif adalah jenis perlindungan yang memungkinkan masyarakat untuk mengajukan keberatan atau menyampaikan pendapat sebelum suatu keputusan pemerintah ditetapkan secara final. Perlindungan ini bertujuan untuk menghindari terjadinya konflik dengan memberikan kesempatan bagi masyarakat.
2) Perlindungan hukum represif adalah bentuk perlindungan yang ditujukan untuk menangani dan menyelesaikan sengketa atau konflik hukum setelah suatu pelanggaran terjadi. Perlindungan ini berfokus pada penanganan masalah yang sudah muncul dengan memberikan sanksi.

Dengan demikian, perbedaan utama antara kedua bentuk perlindungan hukum tersebut terletak pada waktu dan tujuan pelaksanaannya: perlindungan preventif dilakukan sebelum keputusan final untuk mencegah sengketa, sedangkan perlindungan represif dilakukan setelah sengketa muncul untuk menyelesaikannya.

Teori perlindungan hukum menekankan pentingnya hukum

[32] rahardjo, ilmu hukum, 53
[33] Romli, *Perlindungan Hukum* (Palembang: CV. Doki Course and Training, 2024), 165.

yang dibuat dan diterapkan secara benar sebagai jaminan bagi masyarakat. Tujuan utama dari hukum adalah memberikan perlindungan ini. Teori ini sering dikaitkan dengan aliran positivisme, yang menekankan bahwa hukum harus memiliki identitas yang jelas agar dapat berfungsi sebagai pedoman perilaku yang efektif. Namun, hukum juga tak terlepas dari pengaruh politik dan kekuasaan, sehingga hukum sering kali mencerminkan kepentingan pihak yang berkuasa

Hukum bertujuan untuk melindungi kepentingan manusia sebagai subjek hukum agar mereka dapat memperoleh keadilan. Keadilan hanya dapat terwujud apabila prosesnya dijalankan dengan cara yang adil, jujur, bertanggung jawab, serta melalui pertimbangan yang tepat. Pelaksanaan keadilan harus didasarkan pada hukum positif yang relevan dengan situasi nyata masyarakat, agar tercipta kehidupan sosial yang aman dan harmonis. Fungsi hukum adalah melindungi kepentingan masyarakat, dan dalam penegakannya perlu memperhatikan tiga prinsip utama, yaitu:[34]

1) Kepastian Hukum (*Rechtssicherkeit*)

   Dalam kepastian hukum ini menjadikan landasan undang-undang yang tegas bagi penegak hukum saat melaksanakan tugas mereka dalam upaya memberikan perlindungan hukum bagi korban kejahatan.

[34] Ishaq, *Dasar-Dasar Ilmu Hukum* (Jakarta: Sinar Grafika, 2009), 43

2) Kemanfaatan Hukum (*Zeweckmassigkeit*)

Dalam kemanfaatan hukum ini perlindungan hukum bukan hanya diperuntukkan tercapainya kemanfaatan bagi korban kejahatan, melainkan bermanfaat bagi masyarakat.

3) Keadilan Hukum (*Gerechtigkeit*)

Penerapan keadilan dalam perlindungan hukum bagi hak-hak para korban kejahatan tidak sepenuhnya dimiliki, namun hal ini juga dibatasi oleh keadilan yang harus diberikan kepada pelaku kejahatan.

c. Perlindungan Hukum Nasabah

Perlindungan hukum adalah upaya untuk melindungi pihak-pihak yang merasa dirugikan akibat dari ketidakmampuan memenuhi hak-hak mereka karena pihak lain. Pentingnya perlindungan hukum bagi nasabah bank tidak bisa diabaikan, mengingat kerugian yang dialami oleh nasabah dan kebutuhan akan tanggung jawab untuk menjaga hak-hak mereka.

Mengenai perlindungan hukum untuk nasabah bank, Marulak Pardede menyatakan bahwa dalam sistem perbankan Indonesia, perlindungan terhadap nasabah dapat dicapai melalui dua cara:[35]

1) Perlindungan implisit, yang berasal dari pengawasan dan bimbingan bank yang efektif, yang dapat mencegah kebangkrutan bank. Perlindungan ini diperoleh melalui:

a) Undang-undang dan peraturan perbankan

[35] Hermansyah, *Hukum Perbankan Nasional Indonesia* (Jakarta: Kencana, 2011), 145-146

b) Perlindungan yang muncul dari pengawasan dan bimbingan yang dilaksanakan dengan baik di Indonesia

c) Upaya untuk menjaga kelangsungan operasional bank sebagai lembaga secara khusus dan perlindungan terhadap sistem perbankan secara umum

d) Menjaga kesehatan bank

e) Melaksanakan kegiatan usaha sesuai dengan prinsikehati-hatian

f) Metode penyaluran kredit yang tidak merugikan kepentingan bank dan nasabah

g) Memberikan informasi risiko kepada nasabah

b. Perlindungan eksplisit, yaitu perlindungan melalui pendirian sebuah lembaga yang memastikan simpanan masyarakat, sehingga jika sebuah bank mengalami kebangkrutan, lembaga tersebut akan mengembalikan dana publik yang disimpan di bank yang mengalami kegagalan. Perlindungan ini terealisasi melalui pendirian lembaga yang menjamin simpanan publik.

Perlindungan hukum bagi rakyat Indonesia, seperti yang tertuang dalam UUD 1945, secara tegas menyatakan bahwa melindungi seluruh bangsa dan tanah air merupakan tujuan nasional.[36] Perlindungan hukum merupakan hak bagi setiap anggota masyarakat, yang merupakan salah satu tujuan dari Konstitusi Negara Kesatuan Republik Indonesia (NKRI). Konstitusi ini bertujuan untuk menciptakan suatu kesepakatan yang harus

[36] Sekretariat Negara Republik Indonesia, *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945* (Jakarta: Sekretariat Negara Republik Indonesia, 2006), Pembukaan, alinea keempat.

dipatuhi, ditaati, dan dilaksanakan. Hal ini mencerminkan komitmen rakyat Indonesia untuk mengutamakan prinsip-prinsip demokrasi dalam pengambilan keputusan bersama demi kepentingan bangsa.

Tujuan dari perlindungan hukum adalah untuk menjamin kepastian hukum terkait kerugian yang dialami oleh konsumen. Perkembangan teknologi informasi telah menghasilkan produk perbankan berbasis teknologi, yang juga menimbulkan munculnya kejahatan siber. Meskipun kemajuan modern telah mengubah pola perlindungan hukum, tujuan dari perlindungan hukum itu sendiri tetap tidak berubah, itu sendiri tetap sama, yaitu untuk mencapai keadilan, kemanfaatan, dan kepastian hukum yang ideal bagi masyarakat.

2. Konsepsi Perbankan

a. Pengertian bank

Bank merupakan sebuah perusahaan yang mengumpulkan dana dari masyarakat dalam bentuk tabungan, kemudian mengalokasikan uang tersebut kepada orang lain melalui pinjaman atau cara lainnya untuk meningkatkan kualitas hidup banyak individu.[37] Setiap aktivitas perbankan memiliki kemungkinan untuk menghadapi risiko, termasuk risiko penipuan, yang dapat menyebabkan kerugian bagi korban dan menguntungkan pelaku. Fenomena penipuan dalam dunia perbankan sering kali disebabkan oleh ketidakpuasan dari pihak tertentu yang mencari cara untuk mendapatkan keuntungan tanpa mengikuti

[37] Pasal 1 ayat 2 Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan.

prosedur yang benar. Hal ini dapat menyebabkan peningkatan kasus penipuan di industri perbankan, yang jika terus berlanjut, dapat berujung pada kebangkrutan bank tersebut. Oleh karena itu, bank harus beroperasi berdasarkan kepercayaan, sebab mereka memiliki peranan penting dalam perekonomian negara.

Bagi bank yang berdasarkan Prinsip-prinsip syariah sejalan dengan hukum Islam. Prinsip yang diterapkan oleh bank-bank Islam meliputi pembiayaan yang berbasis pada bagi hasil (mudharabah), partisipasi modal (musharakah), dan prinsip perdagangan barang untuk mendapatkan keuntungan (murabahah). Sebelumnya, sistem perbankan di Indonesia hanya dijalankan oleh bank-bank Islam seperti Bank Muamalat Indonesia dan bank perkreditan rakyat (BPR) lainnya. Sesuai dengan Undang-Undang Perbankan yang baru, Nomor 10 Tahun 1998, bank-bank juga dapat menjalankan aktivitas bisnis mereka berdasarkan prinsip syariah, asalkan mereka mematuhi ketentuan yang diatur oleh Bank Indonesia.[38]

Kepercayaan ini sangat penting karena bank dianggap sebagai tempat yang aman untuk menyimpan dan mengatur dana. Untuk menjaga kepercayaan ini, diperlukan upaya yang berkelanjutan dalam menarik dan mempertahankan nasabah. Undang-Undang No. 7 Tahun 1992 tentang Perbankan, yang kemudian diubah oleh Undang-Undang No. 10 Tahun 1998 tentang Perbankan, mengatur pengawasan dan

[38] kasmir, *Bank dan Lembaga Keuangan lainnya*, cet. Ke 12 (Jakarta: RajaGradfindo Pers, 2012), 26.

pengembangan bank oleh Bank Indonesia. Secara umum, bank diwajibkan untuk mengikuti prinsip perbankan yang sehat, mematuhi aturan yang berlaku, serta menghindari praktik atau kegiatan yang dapat merugikan keberlanjutan bank atau kepentingan masyarakat.

b. Fungsi tujuan bank

Bank Indonesia menjalankan operasinya berdasarkan prinsip demokrasi ekonomi dan mengutamakan Perbankan prudensial. Fungsi utamanya adalah mengumpulkan dan mengelola dana publik dengan tujuan mendukung perkembangan nasional untuk meningkatkan pemerataan, pertumbuhan ekonomi, dan stabilitas negara, yang pada akhirnya berkontribusi pada peningkatan kesejahteraan masyarakat (Pasal 2, 3, dan 4 dari Undang-Undang Perbankan No. 10 Tahun 1998 tentang Perbankan).

Berdasarkan pendapat Gusti Ayu, fungsi utama dari sebuah bank adalah mengumpulkan dana dari masyarakat dan menyalurkannya kembali kepada mereka untuk berbagai keperluan, atau berperan sebagai perantara keuangan. Secara lebih spesifik, bank berfungsi sebagai:[39]

1) *Agent Of Turst*: Dasar utama dari kegiatan perbankan adalah kepercayaan, baik dalam pengumpulan maupun penyaluran dana. Masyarakat percaya bahwa uang mereka tidak akan disalahgunakan oleh bank, bahwa pengelolaannya akan dilakukan

[39] Dkk. Purnamawati, I Gusti Ayu, *Bank Dan Lembaga Keuangan Lainnya.* (Yogyakarta: Graha Ilmu, 2014), 10.

dengan benar, bahwa bank tidak akan mengalami kebangkrutan, dan bahwa setoran dapat diambil dari bank pada waktu yang telah dijanjikan.

2) *Agent Of Development:* Aktivitas ekonomi dalam sektor moneter dan sektor riil tidak dapat dipisahkan. Kegiatan perbankan, termasuk pengumpulan dan penyaluran dana, sangat penting untuk kelancaran aktivitas ekonomi di sektor nyata. Kegiatan perbankan yang lancar memungkinkan masyarakat untuk berinvestasi, mendistribusikan, dan mengonsumsi, yang sangat diperlukan untuk pengembangan ekonomi suatu masyarakat.

3) *Agent Of Services*: Selain menyalurkan dana, bank juga menyediakan berbagai layanan perbankan lainnya kepada masyarakat. Layanan yang ditawarkan oleh bank-bank ini sangat berkaitan dengan aktivitas ekonomi secara umum di masyarakat.

c. Jenis- jenis bank

Jenis-jenis bank yang diakui di Indonesia dapat dilihat dalam Pasal 5 (Paragraf 1) Undang-Undang Perbankan, yang membedakan bank menjadi dua jenis: bank umum dan bank perkreditan rakyat.

1) Bank Umum

Sebuah bank umum adalah lembaga keuangan yang menjalankan kegiatan usaha dengan cara konvensional dan/atau berdasar pada prinsip Syariah, serta menyediakan layanan pembayaran. Ini berarti bank umum dapat memberikan semua

layanan perbankan yang ada.

2) Bank Perkreditan Rakyat (BPR)

Bank perkreditan rakyat adalah bank yang menjalankan kegiatan usaha secara konvensional atau berdasarkan prinsip Syariah. Bank ini tidak menyediakan layanan pembayaran. Dengan demikian, layanan perbankan yang ditawarkan oleh BPR jauh lebih terbatas dibandingkan dengan yang disediakan oleh bank umum.[40]

Selain itu bank umum dapat mengkhususkan diri dalam kegiatan tertentu atau fokus pada aktivitas tertentu. Didefinisikan sebagai mengkhususkan diri dalam kegiatan pembayaran jangka panjang, kegiatan untuk pengembangan kerjasama, peningkatan pemilik usaha kecil/ekonomi lemah, pengembangan ekspor non-minyak dan gas, serta pembangunan perumahan.

d. Asas-asas Perbankan

Prinsip hukum diperlukan sebagai dasar untuk kegiatan operasional lembaga perbankan. Prinsip-prinsip yang diakui dalam perbankan Indonesia adalah: Asas Demokrasi Ekonomi, Asas Kepercayaan (*fiduciary Principle*), Asas Kerahasiaan (*Confidential Prinsiple*), Asas Kehati-hatian (*Prudential Principle*).[41]

1) Asas Demokrasi Ekonomi

Salah satu asaa perbankan yang diatur di Indonesia dapat dilihat dari ketentuan Pasal 2 Undang-Undang No. 10/1998, yang

[40] Kasmir, *Dasar-Dasar Perbankan* (RajaGrafindo persada,2014), 20-21.

[41] Djuni S Gazali dan Rachmadi Usman, *Hukum Perbankan* (Jakarta: Sinar Grafika, 2010), 18.

menyatakan bahwa: "Perbankan Indonesia melaksanakan kegiatannya dengan berdasarkan ekonomi demokrasi dengan menggunakan prinsip kehati-hatian." Asas Demokrasi Ekonomi yang dimaksud berdasar pada Undang-Undang Dasar 1945. Hal ini tercantum dalam penjelasan umum dan penjelasan Pasal 2 Undang-Undang No. 10/1998.

2) Asas Kepercayaan (*fiduciary Principle*)

Asas Kepercayaan merupakan suatu prinsip yang menegaskan jika kegiatan perbankan berdasarkan hubungan saling percaya dengan nasabahnya. Bank wajib merahasikan data mereka terutama dengan dana dari masyarakat yang disimpan berdasarkan kepercayaan, sehingga setiap bank harus secara terus-menerus menjaga kesehatan finansialnya dengan mempertahankan dan melestarikan kepercayaan masyarakat. Kesediaan masyarakat untuk menyimpan uang mereka di bank semata-mata didasari oleh keyakinan bahwa mereka akan mendapatkan kembali uang mereka pada waktu yang diinginkan atau sesuai kesepakatan, beserta imbal hasil. Jika kepercayaan nasabah terhadap suatu bank menurun, ada kemungkinan terjadi penarikan besar-besaran terhadap simpanan mereka.[42] Berbagai permasalahan dapat menyebabkan hilangnya kepercayaan terhadap sebuah bank.

[42] Muh Nur eli, *Bank dan Lembaga keuangan* (Graha mulia CV, 2020), 22-23.

3) Asas Kerahasiaan (*Confidential Prinsiple*)

Asas Kerahasiaan merupakan prinsip yang mengharuskan bank untuk melindungi semua hal yang berkaitan dengan keuangan dan informasi lainnya dari nasabah, yang menurut praktik perbankan harus tetap dirahasiakan. Kerahasiaan ini sangat penting bagi bank karena mereka membutuhkan kepercayaan dari masyarakat yang menaruh uang mereka di bank tersebut. Masyarakat hanya akan mempercayakan uang mereka kepada bank atau menggunakan layanan bank jika bank tersebut menjamin tidak akan ada penyalahgunaan atas pengetahuan bank tentang simpanan mereka. Oleh karena itu, bank harus dengan tegas menjunjung tinggi kerahasiaan bank.[43]

4) Asas Kehati-hatian (*Prudential Principle*)

Asas Kehati-hatian merupakan sebuah prinsip yang menyatakan jika ban untuk melaksanakan manfaat dan kegiatan usahanya harus menerapkan prinsip kehati-hatian untuk menjaga keuangan masyarakat yang dipercaya kepadanya. Tujuan dari penerapan asas kehati-hatian ini yaitu untuk memastikan bahwa bank tetap dalam kondisi yang sehat, dengan kata lain untuk menjamin bahwa mereka tetap *likuid* atau *solvent*. Dengan menerapkan prinsip kehati-hatian, diharapkan tingkat kepercayaan masyarakat terhadap perbankan tetap tinggi, sehingga masyarakat

[43] Eli, *Bank dan Lembaga Keuangan*, 23.

akan merasa bersedia dan yakin untuk menyimpan dana mereka di bank.

3. Konsepsi Kejahatan *Phishing*

a. Pengertian *Phishing*

Phishing adalah jenis kejahatan di internet yang termasuk dalam kategori pencurian identitas. Istilah "*phishing*" sebenarnya berasal dari kata "*fishing*," yang menggambarkan penggunaan umpan yang semakin canggih untuk memperoleh informasi keuangan dan kata sandi dari orang-orang yang menjadi sasaran.[44]

Senator Patrick Leahy, dalam pidatonya yang memperkenalkan Undang-Undang Anti-*Phishing* pada tahun 2005, menjelaskan bahwa istilah "*phishing*" berasal dari olahraga "*fishing*," yang mirip dengan teknik melempar umpan pada kail. Dalam konteks *phishing*, "umpan" yang digunakan adalah email atau pesan elektronik yang dirancang untuk meyakinkan korban agar mengungkapkan informasi pribadi atau rahasia mereka. Tujuan utama dari teknik ini adalah untuk berhasil "mengumpulkan" informasi yang diinginkan dari korban.[45]

Phishing adalah jenis kejahatan siber yang terlibat dalam pencurian data, yang dapat menyebabkan kerugian serius bagi korbannya. Para pelaku *phishing* umumnya berpura-pura menjadi perusahaan atau lembaga yang berwenang dan kemudian mengirimkan email yang berisi tautan ke situs web tertentu. Ini dilakukan untuk

[44] Syahdeini, sutan remy, *Kejahatan dan Tindak pidana Komputer*. Jakarta: Pustaka Utama Grafita, 2009, 63.

[45] Syahdeini, sutan remy, *Kejahatan dan Tindak pidana Komputer*,65

menipu korban agar memasukkan informasi sensitif ke dalam situs *phishing*, seperti nama pengguna rekening bank, kata sandi, nomor PIN, dan sebagainya. Setelah data tersebut didapatkan, para pelaku dapat dengan leluasa mencuri saldo rekening korban dan melakukan kejahatan lainnya.[46]

b. Cara Kerja *Phishing*

Berdasarkan penjelasan tentang *phishing*, dapat disimpulkan bahwa tindakan ini dilakukan dengan tujuan untuk menjebak korban oleh pelaku *phishing*. *Phishing* dimanfaatkan untuk mengakses informasi pribadi pengguna dengan memanfaatkan email dan situs web palsu yang menyerupai situs resmi atau asli. Data yang dicari atau diperoleh oleh pelaku *phishing* biasanya adalah kata sandi akun atau nomor kartu kredit korban.

Berikut cara kerja *phishing* berdasarkan sumber ancaman phising, antara lain:[47]

1) *Email*, Serangan dimulai dengan sebuah email yang seolah-olah berasal dari perusahaan yang dikenal korban. Email tersebut meminta korban untuk memperbarui detail mereka dengan mengklik tautan. *Phishing* menggunakan trik dan metode cerdas untuk membuat email tampak palsu. Trik ini membuat orang membagikan informasi pribadi mereka melalui email palsu.

[46] Devie Rahmawati, *Waspada Kejahatan Phishing Attack* (PT Literasi Nusantara Abadi Group, 2024), 10

[47] Suryadi Kurniawan, "*Phising: Pengertian, Cara Kerja dan Langkah Mengatasinya*," niagahoster.ac.id, 2020.

2) *Website,* Di situs web palsu, pengguna diminta memasukkan detail pribadi seperti kata sandi dan detail bank, yang kemudian digunakan untuk mencuri identitas. Peretas menyalin kode dari situs web asli dan mengubahnya agar terlihat seperti situs web asli. Mereka juga menggunakan tautan tersembunyi untuk mendapatkan informasi penting dari orang-orang yang mengunjungi situs tersebut.

3) *Malware,* metode ini membuat karyawan merasa perlu mengunduh berkas untuk menghapus perangkat lunak berbahaya dari komputer mereka.

c. Teknik *Phishing*

Penipu menggunakan berbagai teknik untuk menipu korban, yaitu:[48] Penipu menggunakan berbagai teknik untuk menipu korban, antara lain:

1) *Email Sposing*. Teknik ini sering digunakan oleh penipu, mereka mengirim email kepada jutaan pengguna dengan mengatasinya sebagai lembaga resmi. Email-email ini biasanya meminta nomor kartu kredit, kata sandi, atau unduh formulir tertentu.

2) Penyebaran Melalui Situs Web. Penyebaran melalui situs web adalah salah satu teknik *phishing* yang paling canggih. Teknik ini juga dikenal sebagai "man-in-the-middle," di mana hacker berada di antara situs web resmi dan sistem *phishing*.

[48] Aseh Ginanjar, dkk, Studi Mengenai Serangan Web *Phishing* Terhadap Layanan E-Commerce Menggunakan Metode Proses Forensik Jaringan‖, *JUTEI Vol 2, no. 2* (Oktober 2018): 148, https://jutei. ukdw. ac. id/index. php/jurnal/article/view/11

3) Pesan instan (*chat*). Cara ini melibatkan pengguna yang menerima pesan dengan tautan yang mengarah ke situs web palsu yang tampak dan terasa seperti situs web asli.
4) *Trojan host*. Hackers mencoba masuk ke akun pengguna untuk mengumpulkan data dari komputer lokal. Informasi yang dikumpulkan kemudian dikirim ke penipu.
5) Manipulasi Tautan. Teknik ini melibatkan penipu mengirimkan tautan ke situs web. Saat pengguna mengklik tautan tersebut, mereka akan dialihkan ke situs web *phishing* daripada situs web asli.
6) *Malware* Penipuan: Penipuan *phishing* melibatkan malware yang membutuhkan cara untuk berjalan di komputer pengguna. Malware ini biasanya disertakan dalam email yang dikirimkan ke pengguna oleh pelaku penipuan. Setelah korban mengklik tautan tersebut, malware mulai berfungsi. Malware ini kadang-kadang termasuk dalam file unduhan.

d. *E-banking*

1) Pengertian *E-banking*

Electronic banking merupakan suatu aktivitas layanan perbankan yang menggabungkan antara sistem informasi dan teknologi. *E-banking* meliputi *phone banking*, *mobile banking*, dan *internet banking*. Fungsi penggunaannya mirip dengan mesin ATM, namun sarana yang digunakan berbeda. Seorang nasabah dapat melakukan aktivitas pengecekan saldo rekening, transfer dana

antarrekening atau antarbank, hingga pembayaran tagihan-tagihan rutin bulanan seperti listrik, telepon, kartu kredit, dan berbagai fungsi lainnya. *E-banking* meliputi sistem yang memungkinkannasabah bank, baik individu ataupun bisnis untuk mengakses rekening, melakukan transaksi bisnis, atau mendapatkan informasi produk dan jasa bank melalui jaringan pribadi atau publik, termasuk internet.[49]

2) Cara Kerja *E-banking*

Untuk memanfaatkan teknologi tersebut, seorang nasabah akan dibekali dengan *username* atau user id *untuk* login dan password atau PIN sebagai kode akses untuk memasuki situs web yang di dalamnya Terdapat fasilitas *e-banking*. Selain itu, nasabah bisa login dan melakukan kegiatan perbankan melalui situs web bank yang relevan. *E-banking* sebenarnya tidak baru di internet, tetapi baru saja secara luas diterapkan di Indonesia beberapa tahun terakhir oleh beberapa bank. Bank memberikan layanan perbankan elektronik, atau *e-banking*, untuk memenuhi kebutuhan media transaksi alternatif. Dengan *e-banking*, kita tidak perlu lagi menghabiskan waktu untuk antri di bank atau mesin ATM, karena banyak transaksi perbankan kini bisa dilakukan dengan mudah dan nyaman dari mana saja serta kapan saja melalui jaringan elektronik.[50]

[49] Vyctoria, *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding* (Yogyakarta: Penerbit Andi, 2013), 12.

[50] Vyctoria, *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding*, 13.

BAB III

METODE PENELITIAN

Metode penelitian adalah langkah-langkah yang dilakukan oleh peneliti untuk mengumpulkan data dan informasi yang diperlukan dalam penelitian ilmiah. Metode penelitian merupakan aktivitas yang membutuhkan objektivitas dalam proses, analisis, pengukuran, serta kesimpulan yang dapat memberikan pemahaman. Agar mendapatkan hasil penelitian yang baik, para peneliti mengikuti beberapa langkah berikut:

A. Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian deskriptif hukum normatif. Penelitian hukum normatif atau biasa disebut hukum normatif.[51] Penelitian normatif yuridis ini menempatkan hukum sebagai suatu sistem norma. Ini berarti bahwa penelitian ini mengutamakan untuk menganalisis norma, prinsip, dan peraturan dari hukum serta keputusan pengadilan.[52] Penelitian ini juga mencakup hasil-hasil penelitian terdahulu dan pandangan para tokoh yang berkaitan dengan judul penelitian, yang biasanya dikenal sebagai penelitian kepustakaan.

B. Pendekatan Penelitian

Dalam penelitian ini menggunakan tiga jenis pendekatan, yaitu sebagai berikut:

1. `Pendekatan Perundang-undangan (*Statute Approuch*), pendekatan yang dilakukan dengan cara menalaah pengaturan perundang-undangan terkait

[51] Muhaimin, *Metode Penelitian Hukum*, 2020, 48.
[52] Kristiawanto, *Memahami Penelitian Hukum Normatif*, 2022, 24.

dengan isu hukum yang sedang ingin diteliti.[53] Penelitian ini menggunakan pendekatan undang-undang sebab dalam penelitian ini didalamnya akan menelaah peraturan perundang-undangan yang relevan khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

2) Pendekatan Konseptual (*Conceptual Approuch*), pendekatan ini lahir dari adanya pandangan-pandangan serta doktrin yang berkembang dalam ruang lingkup ilmu hukum. Dalan konteks penelitian ini, pendekatan konseptual digunakan untuk menganalisis perlindungan hukum nasabah terhadap kejahatan *phishing* dalam sistem *e-banking* di indonesia. Dengan menggunakan pendekatan konsep ini juga dapat mengidentifikasi Bagaimana kriteria hukum yang digunakan perihal perlindungan terhadap nasabah, memahami dasar hukum yang digunakan oleh masing masing pengadilan perihal perlindungan hukum terhadap korban.
3) Pendekatan Kasus (*Case Approuch*), pendekatan ini dilakukan dengan cara menelaan kasus-kasus yang berhubungan dengan isu yang dihadapi yang mana kasus-kasus tersebut sudah menjadi putusan pengadilan, tentunya putusan tersebut berkekuatan hukum tetap. Penelitian ini menggunakan pendekatan kasus sebab dalam penelitian ini terdapat kasus nasabah dalam sistem *e-banking* terkait kejahatan phising.

C. Sumber Bahan Hukum

Adapun bahan hukum yang digunakan dalam penelitian ini, yaitu sebagai berikut:

[53] Nur Solikin, Pengantar metode Peneltian Hukum (Pasuruan: CV. Penerbit Qiara Media, 2021), 58.

1. Bahan Hukum Primer

Bahan hukum primer adalah bahan hukum yang memiliki kuat paksa secara umum, seperti peraturan perundang-undangan, serta memiliki kuat paksa untuk pihak yang berkepentingan, seperti kontrak, perjanjian, dokumen hukum, dan putusan hakim.[54] Untuk penulisan dalam penelitian ini dapat digolongkan beberapa bahan hukumprimer yang digunakan, dianataranya yaitu:

a) Undang-Undang Dasar Negara Republik Indonesia 1945
b) Kitab Undang-Undang Hukum Pidana (KUHP)
c) Undang-Undang No. 10 Tahun 1998 tentang Perubahan atas UU No.7 Tahun 1992 tentang Perbankan.
d) Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah
e) Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan
f) Undang-Undang No.19 Tahun 2016 sebagai perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
g) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
h) Peraturan Otoritas Jasa Keuangan No. 38 / POJK.03 / 2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi

2. Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan hukum yang memberikan

[54] Muhaimin, *Metode Penelitian Hukum*: 59

penjelasan terkait bahan hukum primer seperti buku ilmu hukum, jurnal hukum, laporan hukum, serta media cetak dan elektronik.[55] Untuk penulisan dalam penelitian ini dapat digolongkan beberapa bahan hukum primer yang meliputi buku, termasuk skripsi, jurnal, serta disertasi yang berkaitan dengan perlindungan hukum terhadap nasabah.

D. Teknik Pengumpulan Bahan Hukum

Dalam penelitian ini menggunakan strategi pengumpulan bahan hukum melalui penelitian kepustakaan. Teknik pengumpulan bahan hukum ini bersumber dari pengumpulan tulisan dari sumber-sumber atau bahan-bahan yang berhubungan dengan buku, undang-undang, peraturan Republik Indonesia, serta studi dokumen atau arsip yang berhubungan dengan masalah yang akan dibahas dalam penulisan skripsi ini.

E. Teknik Analisis Bahan Hukum

Analisis terhadap bahan hukum yang digunakan dalam penelitian hukum normatif dilakukan dengan langkah-langkah berikut:

1. Menentukan fakta hukum dan menghilangkan informasi yang tidak perlu.
2. Mengumpulkan sumber hukum dan non-hukum terkait topik hukum tersebut.
3. Menganalisis masalah hukum berdasarkan informasi yang telah dikumpulkan.
4. Menyimpulkan berdasarkan pertimbangan hukum dalam argumen yang diajukan.

[55] Peter Muhammad Marzuki, *Penelitian Hukum* (Jakarta: Kencana: Prenada Media Group, 2017): 181.

5. Memberikan rekomendasi berdasarkan alasan yang disampaikan.

Hasil analisis bahan hukum dijelaskan dengan menggunakan teknik deduktif, mulai dari isu yang luas hingga spesifik. Kemudian hasil tersebut dipelajari dan ditransformasikan menjadi preskripsi, dengan tujuan mencapai hasil yang diharapkan, yaitu menyelesaikan perumusan masalah saat ini.

F. Keabsahan Bahan Hukum

Keabsahan bahan hukum dalam penelitian normatif ini merupakan salah satu bentuk validitas dan kebenaran sumber hukum yang digunakan dalam penelitian, apakah dalam penelitian tersebut sudah benar atau sesuai dengan peraturan yang berlaku. Sehingga keabsahan hukum ini sangat penting sebab juga akan menjadi acuan sejauh mana sumber-sumber hukum yang digunakan dalam penelitian tersebut serta juga memastikan bahwa analisis hukum yang dilakukan dalam penelitian tersebut telah berdasarkan pada sumber yang sah, relevan, dan sesuai dengan hukum yang berlaku. Apabila dalam penelitian menggunakan bahan hukum yang tidak sah atau tidak relevan maka akan dapat menambah argumentasi hukum dan hasil penelitian. Maka dari itu, penting untuk selalu menguji keabsahan sumber bahan hukum dalam setiap penelitian.

G. Tahap Penelitian

Pada bagian ini peneliti akan memaparkan terkait rencana tahapan dalam penelitian secara sistematis, mulai dari pra riset (sebelum melakukan penelitian), riset (saat penelitian), dan pasca riset (setelah melakukan

penelitian), hingga tahap akhir yaitu penulisan laporan. Berikuta beberapa tahapan penelitian yang akan dilakukan peneliti:

1. Pra Riset
    a) Mengidentifikasi isu hukum yang akan diteliti
    b) Menetukan judul penelitian
    c) Mempersiapkan bahan-bahan rujukan yang akan dijadilan pedoman dalam penelitian, termasuk jurnal, dan karya ilmiah lainnya.
2. Riset
    a) Memahami latar belakang serta inti permasalahan yang akan diteliti
    b) Mengumpulkan bahan hukum sesuai rujukan yang relevan dengan fokus masalah yang akan diteliti.
    c) Menganalisis bahan sesuai dengan urutan analisis agar ditemukan hasil yang akurat.
    d) Merangkum bahan hukum yang telah ditemukan dalam penelitian untuk nantinya disusun menjadi sebuah penelitian yang terstruktur.
3. Pasca Riset
    a) Merangkai hasil dari temuan yang dilakukan pada tahap riset untuk disesuaikan pada pokok permasalahan penelitian.
    b) Menarik kesimpulan.

BAB IV

PEMBAHASAN

A. Bentuk Kejahatan *Phishing* Dalam Aplikasi *E-banking* di Indonesia

1. Bentuk-bentuk Kejahatan *Phishing* dalam Sistem *E-banking*

Dalam praktiknya, tindakan penipuan *phishing* dapat dibedakan menjadi beberapa bentuk utama berdasarkan cara yang digunakan oleh pelaku, yaitu:[56]

a. *Email Phishing*

Metode ini melibatkan pengiriman email yang tampak resmi dari bank atau lembaga keuangan. Email tersebut biasanya berisi peringatan palsu tentang akun yang bermasalah, permintaan verifikasi data, atau tawaran promosi yang mengarahkan korban untuk mengklik tautan tertentu. Setelah korban mengklik tautan tersebut, mereka akan diarahkan ke situs web palsu yang menyerupai situs resmi bank, di mana mereka diminta untuk memasukkan informasi pribadi mereka.[57]

b. SMS dan *WhatsApp Phishing (Smishing*)

Metode ini menggunakan pesan singkat (SMS) atau aplikasi pesan seperti WhatsApp untuk mengirimkan tautan berbahaya. Pesan-pesan ini sering menyamar sebagai bank dan memberi tahu korban bahwa akun mereka telah diblokir atau ada transaksi mencurigakan

[56] Dika Agustian Akbar, Muhammad Rahdian Ega Kurnia, R.M. Genggam Satoe Bintang, dan Rahmat Purwoko, "Analisis Web *Phishing* Menggunakan Metode OSCAR Forensic (Studi Kasus: Follower Instagram Gratis)," Jurnal Teknik Informatika, Vol. 3, No. 1 (Februari 2024), 18–24.

[57] Justin Petelka, Yixin Zou, dan Florian Schaub, "Put Your Warning Where Your Link Is: Improving and Evaluating Email *Phishing* Warnings," *Proceedings of the CHI Conference on Human Factors in Computing Systems* (CHI 2019), Glasgow, Scotland, 4–9 Mei 2019 (New York: ACM, 2019), 1–15, https://doi.org/10.1145/3290605.3300748

yang harus segera dikonfirmasi melalui tautan yang disediakan. Setelah korban mengklik tautan tersebut, mereka akan diarahkan ke situs web palsu yang meminta kredensial login dan informasi pribadi lainnya.

c. Voice *Phishing* (*Vishing*)

Dalam metode ini, pelaku melakukan panggilan telepon kepada korban dengan berpura-pura menjadi karyawan bank atau pejabat keuangan lainnya. Pelaku berusaha meyakinkan korban untuk memberikan informasi penting seperti nomor kartu kredit, kode kata sandi sekali pakai (OTP), atau data pribadi lainnya. Teknik ini sering kali digunakan dengan nada mendesak untuk membuat korban merasa panik dan segera memberikan informasi yang diminta tanpa berpikir panjang.[58]

d. Situs Web Palsu

Para pelaku kejahatan sering menghasilkan situs web palsu yang menyerupai tampilan laman resmi bank atau aplikasi perbankan. Situs-situs ini bisa muncul dalam hasil pencarian Google, disebarkan melalui iklan *online,* atau dikirim melalui email atau SMS. Jika korban tidak berhati-hati dan memasukkan informasi mereka, data tersebut akan langsung jatuh ke tangan pelaku untuk disalahgunakan.

e. Media Sosial *Phishing*

Kejahatan *phishing* juga sering terjadi di media sosial, di mana

[58] Petelka, Zou, dan Schaub, *Put Your Warning*, 10.

pelaku membuat akun palsu yang menyerupai akun resmi bank. Akun-akun ini kemudian digunakan untuk menghubungi korban, menawarkan bantuan, atau mengarahkan mereka untuk mengunjungi tautan tertentu yang sebenarnya adalah situs *phishing*.

Dengan adanya berbagai bentuk tersebut, jelas bahwa *phishing* merupakan kejahatan yang dinamis dan adaptif. Ketika sistem keamanan perbankan makin canggih, strategi yang digunakan oleh para pelaku juga semakin canggih. Berdasarkan ketentuan hukum Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (OJK) memiliki tanggung jawab mengawasi industri jasa keuangan, termasuk perbankan, untuk memastikan penerapan prinsip kehati-hatian dan perlindungan konsumen dari berbagai risiko, termasuk yang disebabkan oleh kejahatan siber seperti *phishing*. Peran OJK diatur agar lembaga keuangan melaksanakan manajemen risiko teknologi informasi yang memadai untuk mencegah dan mengurangi kejahatan *phishing*.

Selain itu, Peraturan OJK No. 38/PJOK. 03/2016 mewajibakan penerapan manajemen risiko dalam penggunaan teknologi informasi oleh lembaga perbankan untuk menerapkan sistem keamanan teknologi informasi yang mencakup control administrative, teknis dan procedural untuk menghindari pembocoran data nasabah serta kejahatan digital yang bisa mengancam keamanan transaksi *e-banking*.

Menurut tinjauan hukum, tindakan *phishing* dalam aplikasi *e-banking* merupakan pelanggaran yang diatur dalam Undang-Undang

Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016. Pasal 30 Undang-Undang ITE menyatakan larangan bagi siapapun untuk secara sengaja dan tanpa izin mangakses sistem elektronik milik pihak lain, sedangkan Pasal 35 mengatur larangan untuk memanipulasi data elektronik demi keuntungan pribadi. Dengan demikian, praktik *phishing* adalah sebuah pelanggaran hukum yang dapat dikenakan sanksi pidana berupa penjara dan denda sesuai yang diatur dalam Pasal 46 dan Pasal 51 Undang-Undang ITE.[59]

Selain itu, bentuk kejahatan *phishing* juga berkaitan erat dengan pelanggaran perlindungan data pribadi seperti yang diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Ketika data pribadi nasabah disalahgunakan oleh pihak yang tidak bertanggung jawab, hal ini tidak hanya merugikan korban secara finansial, tetapi juga mengancam hak konstitusi setiap warga negara yang dijamin dalam Pasal 28G ayat (1) UUD 1945 mengenai perlindungan pribadi.[60]

Dengan demikian, bentuk-bentuk kejahatan *phishing* dalam aplikasi *e-banking* di Indonesia meliputi berbagai modus operandi digital, mulai dari pengiriman tautan palsu, situs web yang tidak benar, pesan email yang menyesatkan, hingga distribusi malware. Semua tindakan kejahatan ini tidak hanya merugikan nasabah secara materiil tetapi juga menyebabkan

[59] Sekretariat Negara Republik Indonesia, Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[60] Sekretariat Negara Republik Indonesia Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 28G ayat (1)

kerugian immateril berupa hilangnya keamanan dan kepercayaan dalam sistem perbankan digital. Hal ini menekankan pentingnya penegakan hukum yang konsisten dan perlindungan hukum yang efektif untuk melindungi nasabah sebagai konsumen layanan keuangan digital.

2. Analisis Bentuk Kejahatan *Phishing* Dalam Aplikasi *E-banking* di Indonesia

Perkembangan teknologi digital telah memberikan dampak besar pada dunia perbankan elektronik (*e-banking*). Transformasi ini memungkinkan akses mudah kelayanan keuangan tanpa batasan waktu dan tempat.[61] Namun, kemajuan ini juga diikuti dengan munculnya berbagai bentuk kejahatan siber, salah satunya adalah *phishing*. Dalam sistem *e-banking*, *phishing* menjadi ancaman serius karena dapat menipu nasabah untuk secara sukarela menyerahkan data pribadi dan finansial mereka kepada pelaku kejahatan *phishing*.

Bentuk bentuk *phishing* dalam *e-banking* mencakup pengiriman tautan atau situs palsu yang menyerupai halaman masuk bank, penyebaran malware melalui aplikasi atau tautan, dan komunikasi elektronik yang menipu seperti email, SMS, atau panggilan telepon. Para pelaku *phishing* biasanya menipu korban agar secara sukarela memberikan data sensitif, yang kemudian digunakan untuk mengakses akun mereka secara ilegal dan melakukan transaksi yang tidak sah, yang mengakibatkan kerugian finansial yang besar bagi nasabah.

[61] Budi Rhardjo, *Keamanan Sistem Informasi Berbasis Internet* (Bandung: Informatika, 2018), 21.

Kejahatan *phishing* pada dasarnya memenuhi unsur tindak pidana penipuan sebagaimana diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana, yang menyatakan bahwa "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum,dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun".[62] Dengan demikian, unsur penipuan dalam Pasal 378 KUHP dapat ditemukan dalam kasus *phishing*, karena pelaku memanfaatkan kebohongan melalui sistem elektronik untuk menggerakkan korban agar menyerahkan data pribadinya.

Selain ketentuan dalam KUHP, tindakan *phishing* juga diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016, pada Pasal 30 ayat (1) yang menyatakan larangan bagi siapa pun untuk mengakses sistem elektronik milik orang lain tanpa izin. Pelaku *phishing* yang dengan sengaja mendapatkan dan menggunakan data elektronik korban untuk keuntungan pribadi juga melanggar 35 UU ITE, yang melarang setiap orang untuk memanipulasi, membuat, mengubah, atau menghapus informasi elektronik atau dokumen elektronik dengan tujuan untuk membuat seolah-olah data tersebut benar

[62] Andi Hamzah, *Delik-Delik Tertentu (Speciale Delicten) di Dalam KUHP*, 100.

atau sah. Pelanggaran terhadap pasal-pasal tersebut dapat dikenakan sanksi penjara dan denda sebagaimana tercantum dalam pasal 46 dan 51 UU ITE.

Bentuk penipuan *phishing* dalam aplikasi *e-banking* di Indonesia sangat beragam dan terus berkembang seiring dengan kemajuan teknologi serta pola pengguna nasabah. Bentuk yang paling umum adalah *phishing* melalui email, dimana pelaku mengirimkan email palsu yang terlihat berasal dari bank dan mengarahkan korban ke situs web palsu ntuk memasukkan data pribadi mereka. Selain itu, ada juga *phishing* melalui SMS dan WhatsApp yang memanfaatkan pesan teks dan aplikasi pesan instan untuk menyebarkan tautan berbahaya dengan modus memberikan peringatan palsu atau informasi akun yang bermasalah. *Phishing* suara (vishing) melibatkan panggilan telepon dari pelaku yang menyamar sebagai bank untuk menipu korban agar memberikan data sensitive. Metode lain termasuk membuat situs web palsu yang menyerupai portal perbankan resmi, serta *phishing* melalui media sosial, dimana akun-akun palsu dibuat untuk menipu nasabah.[63]

Otoritas Jasa keungan (OJK) memiliki peran penting sebagai pengawas dalam melindungi keamanan sistem perbankan dari ancaman penipuan elektronik. OJK menetapkan kewajiban manajemen risiko teknologi informasi dalam Peraturan OJK No. 38/PJOK. 03/2016 dan Surat Edaran OJK no. 29 Surat Edaran otoritas Jasa Keuangan. 03/2022, yang mewajibakan bank untuk menerapkan control administrative, teknis,

[63] Cut Mutia, "Analisis Penipuan Digital teknik *Phishing* Terhadap Layanan Mobile Banking," *jurnal Tranformasi Bisnis Digital (JUTRABIDI),* Vol. 1, No. 4 (Juli 2024), 8.

teknis, dan prosuderal agar tidak terjadi kebocoran data nasabah dan mencegah kejahatan digital. Tujuan dari manajemen risiko ini aalah untuk melindungi nasabah dari kerugian material dan juga menjaga stabilitas industri keuangan serta kepercayaan masyarakat.[64] Perlindungan hukum mencakup tidak hanya aspek pidana tetapi juga tanggung jawab perdata bamk terhadap nasabah yang menjadi korban penipuan, sesuai dengan Undang-Undang perlindungan Konsumen dan Undang-undang Perbankan, untuk memastikan hak-hak nasabah terpenuhi, termasuk mekanisme penyelesaian sengketa baik secara internal maupun melalui jalur hukum.

Modus operandi yang beragam ini menunjukkan bahwa kejahatan *phishing* bersifat adaptif dan dinamis, selalu menyesuaikan diri dengan perkembangan teknologi serta perilaku masyarakat digital. Sebuah laporan dari Otoritas Jasa Keuangan (OJK) mengindikasikan bahwa kasus *phishing* pada layanan *e-banking* di Indonesia telah meningkat seiring dengan bertambahnya penggunaan layanan keuangan digital, khususnya selama pandemi COVID-19 ketika transaksi *online* menjadi pilihan utama masyarakat.

Dari segi hukum, kejahatan *phishing* tidak hanya menimbulkan kerugian material berupa hilangnya dana pelanggan, tetapi juga kerugian immaterial seperti berkurangnya keamanan dan kepercayaan publik terhadap sistem perbankan digital. Selain itu, tindakan *phishing* juga melanggar hak perlindungan data pribadi yang diatur dalam Undang-

[64] Surat Edaran Otoritas Jasa Keuangan Nomor 21/SEOJK.03/2017 tentang *Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum*.

Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pasal 4 UU ini menegaskan bahwa setiap orang berhak atas perlindungan data pribadinya, sedangkan Pasal 65 memberikan sanksi pidana bagi siapa saja yang secara ilegal mengungkapkan dan menggunakan data pribadi tanpa izin pemiliknya. Oleh karena itu, pelaku *phishing* dapat diadili tidak hanya berdasarkan ketentuan Kitab Undang-Undang Hukum Pidana dan UU ITE, tetapi juga berdasarkan UU PDP.

Aspek psikologis dan kesadaran pengguna juga merupakan faktor penting dalam risiko serangan *phishing*. Kurangnya edukasi nasbah dan pemahaman tentang metode *phishing*, serta ketertarikan nasabah terhadap tawaran palsu dimedia sosial atau email, menciptakan kesadaran nasabah dan pendidikan yang berkelanjutan adalah strategi kunci untuk menurangi keberhasilan serangan *phishing* disektor perbankan digital.

Dengan demikian, *phishing* melaui *e-banking* merupakan kejahatan yang terus berkembang dan beragam, yang mengakibatkan kerugian baik secara materi maupun non-materi. Regulator seperti Otoritas Jasa keuangan (OJK) sereta peraturan seperti Kitam Undang-Undang Hukum Pidana, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dan Undang-Undang Perlindungan Data Pribadi (UU PDP) membentuk kerangka hukum yang kompleks untuk menangani dan mencegah kejahatan ini. Meski demikian, tantangan dalam penegakan hukum seperti kesulitan dalam mengidentifikasi pelaku, koordinasi antar lembaga, dan rendahnya kesadaran masyarakat masih menjadi hambatan utama. Oleh

karena itu, perlindungan hukum yang efektif tidak hanya memerlukan regulasi dan penegakan yang konsisten, tetapi juga peran aktif dari bank sebagai penyedia layanan dan pendidikan pengguna dan berkelanjutan.

B. Akibat Kejahatan *Phishing* Terhadap Nasabah Pengguna Layanan *E-banking*

Penggunaan layanan internet banking dapat menimbulkan berbagai faktor yang merugikan bagi nasabah. Salah satu penyebab utama yang kelemahan nasabah adalah rendahnya kesadaran masyarakat mengenai hak-hak mereka. Meskipun *e-banking* memberikan kenyamanan, ada pula risiko yang membuat nasabah berada diposisi lemah, seperti pengurangan saldo rekening tanpa sepengetahuan mereka, pencurian data pribadi oleh pihak yang tidak bertanggung jawab, dan transfer uang melalui *e-banking* yang tidak masuk kerekening tujuan.

Kasus kejahatan *phishing* yang muncul karna penyalahgunaan data pribadi oleh pihak yang tidak berwenang masih sering terjadi. Misalnya, masih banyak panggilan, pesan teks, atau email dari orang yang tidak dikenal atau yang mengaku mewakili institusi resmi yang menawarkan sesuatu. berbagai manfaat dengan tujuan menipu calon korban untuk memberikan data pribadi mereka. Ketika nasabah menginput data dan kata sandi mereka ke situs palsu, informasi tersebut akan ditangkap oleh penipu dan digunakan untuk merugikan nasabah, terdapat beberapa akibat dari kejahatan *phishing*.[65]

[65] Clara Nervia, Kresentia Aiko Wardhana, Pricilia Angel Sie, Talitha Livia Talim, dan Waynehard Brayne Hizkia, "Analisis Yuridis terhadap Kejahatan Phising dalam Sistem Perbankan Digital melalui Scam Link Berbahaya," IKON*: Jurnal Ilmu Hukum, Vol. 29, No. 2* (Agustus 2025), 13, https://doi.org/10.37817/ikon.v29i1

1. **Kerugian Finansial**

Dari beberapa kejahatan *phishing* salah satunya merupakan kerugian finansial yakni hilangnya keseluruhan maupun sebagian dana nasabah akibat kejahatan tersebut. Nasabah yang menjadi sasaran *phishing* dapat kehilangan uang mereka akibat transaksi illegal yang dilakukan oleh pelaku. Dalam beberapa kasus, korban bahkan kehilangan seluruh saldo rekening mereka sebelum menyadari bahwa mereka telah ditipu. *Phishing* dapat menimbulkan kerugian finansial secara langsung, misalnya korban *phishing* bisa kehilangan uang secara langsung jika mereka memberikan informasi rekening bank atau kartu kredit kepada penipu. Penipu bisa menguras saldo atau melakukan transaksi yang tidak diizinkan menggunakan data tersebut. Selain itu, korban juga bisa kehilangan uang secara tidak langsung jika datanya dijual ke pihak lain yang menggunakan informasi itu untuk melakukan tindakan kriminal lainnya, seperti pencurian identitas.[66]

Salah satu contoh yang ada yaitu pada web page KOMPAS.Com yang ditulis oleh Aji YK Putra, Teuku Muhammad Valdy Arief terdapat pelaku kejahatan *Phishing* yang berhasil ditangkap akibat dari kejahatannya tersebut. Hal tersebut mengakibatkan kerugian terhadap korban sebesar Rp 1,4 miliar rupiah setelah pelaku berhasil mengambil alih *mobile banking* targetnya melalui Whatsapp dengan cara mengirimkan

[66] Devie Rahmawati, *Waspada Kejahatan Phishing Attack* (Jakarta: PT Literasi Nusantara Abadi Group, 2024), 12

file berbentuk aplikasi.[67] Kasus ini menunjukkan betapa seriusnya dampak kejahatan *phishing* yang memanfaatkan kelalaian korban dalam menjaga keamanan data pribadinya secara digital.

Selain itu, kasus nyata dapat dilihat dalam laporan Otoritas Jasa Keuangan (OJK) pada bulan februari 2025, yang mencatat adanya 42.257 laporan penipuan transaksi keuangan dengan total kerugian mencapai Rp 700,2 miliar, yang sebagian besar dari modus *phishing* dan rekayasa sosial yang menargetkan pengguna layanan *e-banking*.[68] Fakta ini menunjukkan bahwa rendahya literasi digital dikalangan masyarakat tetap menjadi faktor yang meningkatkan kerugian finansial akibat kejahatan *phishing* di Indonesia.

Pada dasarnya phising melibatkan tindak kriminal dimana pelaku menyamar sebagai individu atau entitas terpercaya melalui pesan elektronik guna memperoleh informasi pribadi dan rahasia milik korban. Teknik ini umumnya berkaitan dengan metode rekayasa sosial. Berdasarkan Undang-Undang No.19 Tahun 2016 sebagai perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, disebutkan bahwa setiap orang dilarang untuk dengan sengaja dan tanpa hak, atau secara melawan hukum, mengakses komputer dan/atau sistem elektronik dalam bentuk apa pun yang mencakup pelanggaran, penetrasi,

[67] Aji YK Putra, Teukyu Muhammad Valdy Arief, "Pelaku *Phishing* Bermodus APK via WhatsApp Ditangkap, Kuras Rp 1,4 M Tabungan Korban" 18 Oktober, 2025, https://regional.kompas.com/read/2023/10/30/183238278/pelaku-*phishing*-bermodus-apk-via-whatsapp-ditangkap-kuras-rp-14-m-tabungan

[68] Otoritas Jasa Keuangan (OJK), "OJK Terima 42.257 Laporan Penipuan, Total Kerugian Korban Tembus Rp700,2 Miliar," *Infobanknews.com*, 18 Oktober 2025, https://infobanknews.com/ojk-terima-42-257-laporan-penipuan-total-kerugian-korban-tembus-rp7002-m/

melewati, atau membobol sistem keamanan. Oleh sebab itu, phising dianggap sebagai tindakan kriminal yang melanggar hukum, dan menurut pasal ini, dapat dikenai hukuman penjara hingga 8 tahun dan/atau denda sebesar Rp800.000.000,00 (delapan ratus juta rupiah). Hal ini mempperlihatkan betapa tegasnya sanksi yang diberlakukan guna menjaga kemanan serta integritas sistem elketronik terhadap kejahatan seperti *phishing*.[69]

Dengan demikian, bahwa kerugian finansial akibat kejahatan *phishing* terhadap nasabah dalam sistem *e-banking* tidak hanya mencakup kehilangan dana secara langsung, tetapi juga berdampak luas terhadap stabilitas sistem keuangan digital dan kepercayaan nasabah terhadap perbankan. Oleh karena itu, sangat penting bagi lembaga perbankan dan pemerintah untuk memperbaiki sistem keamanan elektronik, meningkatkan pemahaman digital masyarakat, serta menerapkan sanksi hukum dengan tegas kepada pelaku kejahatan *phishing* agar tercipta perlindungan hukum yang efisien bagi para nasabah yang menjadi korban.

2. Kerugian Non Finansial

a. Kurangnya kepercayaan nasabah

Percaya kepada nasabah membutuhkan waktu untuk terbentuk, berkembang perlahan, dan terus menumpuk. Dalam konteks perbankan, kepercayaan nasabah sangat penting karena dapat memperkuat hubungan antara nasabah dan bank. Kepercayaan nasabah adalah dasar

[69] Akhmad Fery Hasanudin, A Basuki Babussalam, "Upaya Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking" *Gagasan Hukum*, Vol. 6, no. 01 (2024):

dari bisnis perbankan. Membangun kepercayaan nasabah agar mereka merasa aman dalam bertransaksi dengan bank sangat penting untuk menciptakan dan menjaga hubungan dengan nasabah.[70] Oleh karena itu, kepercayaan pelanggan merupakan faktor penting yang mendorong pelanggan untuk melakukan transaksi perbankan. Apabila terjadi *phishing*, kepercayan ini akan menurun karena nasabah merasa sistem perbankan sudah tidak aman lagi untuk digunakan. Menurunnya kepercayaan nasabah ini berpotensi menghambat perluasan penggunaan layanan perbankan elektronik dimasyarakat.

Kepercayaan nasabah sangat penting dalam dunia perbankan. *Phishing* adalah salah satu kejahatan yang dapat membahayakan keamanan simpanan nasabah disektor perbankan. Selain itu, risiko ini bisa mengganggu upaya bank untuk mempertahankan citra mereka dan mendapatkan kepercayaan nasabah. Hubungan yang baik antara bank dan nasabah sangat bergantung pada rasa aman dan kepercayaan yang mereka miliki. *Phishing* telah menimbulkan kerugian besar bagi masyarakat secara keseluruhan karena dampak materinya akibat pencurian data atau informasi bank, yang dapat menyebabkan masalah jangka panjang seperti kerusakan reputasi atau kesulitan dalam mengakses layanan keuangan. Praktik ini juga bisa menurunkan kepercayaan publik terhadap transaksi digital, sehingga memperlambat

[70] P. Robbins, *Organizational Behavior*, ed. ke-10, alih bahasa Drs. Benyamin Molan (Jakarta: Salemba Empat, 2003), 112.

adopsi teknologi baru.[71]

Dari sudut pandang praktis, bank dan lembaga keuangan harus menyadari bahwa hanya mengandalkan keamanan teknis tidaklah memadai. Meningkatkan pemahaman digital nasabah, transparansi tentang insiden keamanan, dan komunikasi yang jelas mengenai langkah-langkah pencegahan sangat penting untuk membangun kembali kepercayaan. Ketika pelanggan melihat bahwa bank berupaya untuk melindungi mereka, rasa percaya dapat meningkat meskipun ancaman siber terus berkembang.

Kurangnya kepercayaan nasabah akibat kejahatan *phishing* sangat terkait dengan tanggung jawab bank untuk menjaga keamanan sistem elektronik banking. Berdasarkan Pasal 29 ayat (2) Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, bank diwajibkan untuk menjaga kepercayaan publik dengan melaksanakan aktivitas usaha secara sehat. Ketika sistem keamanan *e-banking* tidak mampu melindungi data nasabah, maka kepercayaan publik terhadap lembaga keuangan tersebut secara tidak langsung terancam, sehingga bank wajib memperkuat perlindungan hukum dan mekanisme pemulihan bagi korban.[72]

[71] Putu Davis Justin Thenata, Ryan Jovan Susanto, Jeanette Olivia Kurniawati, dan Jessica Carol Lee, "Analisis Tanggung Jawab Hukum Terhadap Keamanan Perbankan dan Nasabah dalam Kasus *Phishing*," *Cerdika: Jurnal Ilmiah Indonesia*, Vol. 5, No. 4 (April 2025)

[72] Sekretariat Negara Republik Indoensia Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, Pasal 29 ayat (2)

b. Akibat Psikologis Terhadap Nasabah

Akibat kejahatan *phishing*, nasabah bisa mengalami stress dan trauma. Nasabah cenderung mengalami perasaan takut, rasa bersalah, hingga Depresi terjadi karena menjadi korban penipuan. Mereka juga merasa tidak aman dan khawatir akan data serta privasi mereka dalam bertransaksi perbankan *online*. Tekanan dan trauma ini dapat berdampak negatif pada kesehatan mental dan fisik korban. Beberapa dampak psikologis yang mungkin muncul karena kejahatan phising terhadap nasabah adalah:[73]

1) Stress. Korban *phishing* mengalami stress karena khawatir data pribadi mereka akan dimanipulasi oleh pelaku, atau karena tekanan dari pihak yang terlibat dalam data yang diambil, seperti bank.
2) Trauma. Korban *phishing* bisa mengalami trauma yang membuat mereka takut atau ragu untuk menggunakan layanan *e-banking* kembali.
3) Depresi. Korban *phishing* bisa mengalami depresi karena merasa bersalah karena menjadi korban penipuan *online*. Depresi juga bisa disebabkan oleh kerugian finansial yang besar atau hilangnya kepercayaan dari orang-orang di sekitar mereka.
4) Kecemasan.Korban *phishing* mungkin merasa cemas karena tidak tahu cara menyelesaikan masalah akibat *phishing*, atau karena takut

[73] Rahmawati, *Waspada Kejahatan Phishing Attack*, 14.

menjadi korban *phishing* lagi dimasa mendatang.[74]

Tindakan *phishing* tidak hanya sebatas mengubah situs web atau email untuk menipu korban, tetapi juga melibatkan kebohongan yang bertujuan untuk menipu korban yang pada akhirnya mengakibatkan kerugian.

Perlindungan hukum bagi pengguna layanan perbankan, berdasarkan Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan ("UU 10/1998"), mencakup beberapa aspek penting bagi nasabah:[75]

1) Penyampaian Informasi Mengenai Risiko Kerugian: UU 10/1998 mengatur bahwa bank wajib memberikan informasi kepada nasabah mengenai kemungkinan risiko kerugian yang dapat timbul dari transaksi yang dilakukan. Hal ini bertujuan untuk memastikan nasabah mendapatkan informasi yang jelas mengenai kondisi keuangan bank dan risiko yang mungkin mereka hadapi.
2) Kerahasiaan Bank: UU 10/1998 menjamin kerahasiaan bank yang meliputi semua informasi tentang nasabah dan simpanan mereka. Bank harus menjaga kerahasiaan ini terkecuali dalam situasi yang diatur secara jelas dalam undang-undang, seperti untuk kepentingan pajak, proses hukum, atau dengan persetujuan tertulis dari nasabah.
3) Lembaga Penjamin Simpanan: UU 10/1998 mewajibkan setiap bank

[74] Liputan6.com. (2020). Tak Hanya *Phishing*, ini 9 Metode Serangan Siber yang Perlu Diketahui. https://www.liputan6.com/cek-fakta/read/5280986/tak-hanya-phising-berikut-ini-9-metode-serangan-siber-yang-perlu-diketahui

[75] Sekretariat Negara Republik Indonesia Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan

untuk menjamin dana publik yang disimpan di sana. Hal ini dilakukan melalui pendirian Lembaga Penjamin Simpanan (LPS), yang bertugas memberikan jaminan untuk simpanan nasabah jika suatu bank mengalami kesulitan keuangan

Selain tiga aspek ini, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen ("UU 8/1999") juga memberikan perlindungan tambahan bagi nasabah perbankan.[76] Undang-undang ini menetapkan standar perilaku yang harus dipatuhi oleh penyedia layanan perbankan, termasuk kewajiban untuk memberikan informasi yang jujur, tidak diskriminatif, serta melindungi nasabah dari klausul standar yang merugikan.

Dengan demikian, melalui seperangkat undang-undang ini, pemerintah Indonesia berusaha untuk memastikan bahwa nasabah perbankan mendapatkan perlindungan yang memadai saat menggunakan layanan perbankan, mulai dari informasi yang jelas mengenai risiko kerugian, menjaga kerahasiaan data pribadi mereka, hingga jaminan atas simpanan mereka di bank.

3. Analisis Akibat kejahatan *Phishing* Terhadap Nasabah Pengguna Layanan *E-banking*

Salah satu dampak paling jelas dari kejahatan *phishing* adalah kerugian finansial bagi nasabah. *Phishing* adalah sebuah tindakan kriminal yang melibatkan pencurian data dan akses tanpa ijin, dapat menyebabkan

[76] Sekretariat Negara Republik Indonesia Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

nasabah kehilangan saldo akun mereka baik secara langsung maupun tidak langsung. Laporan dari Otoritas Jasa Keungan (OJK) menunjukkan bahwa kerugian yang dialami masyarakat mencapai ratusan juta miliar rupiah akibat skema *phishing* dan rekayasa sosial. Dalam praktiknya, pelaku mengakseskan akun nasabah melalui data yang diperoleh dari situs web palsu, email, atau pesan teks, menipu korbannya untuk membocorkan informasi rahasia, yang memungkinkan mereka melakukan transaksi illegal atau menarik dan tanpa sepengetahuan nasabah.[77]

Dari sudut pandang hukum pidana, kegiatan ini diatur oleh Pasal 32 UU ITE, yang melarang akses illegal terhadap sistem elektonik, serta Pasal 30 yang melarang maipulasi data elektronik (Undang-Undang No. 19 tahun 2016). Hukuman pidana maksimal dapat mencapai delapan tahun penjara dan denda sebesar 800 juta, sebagai bentuk penguatan hukum terhadap kejahatan ini yang sering menimbulkan kerugian besar. Selain sanksi pidana, kerugian finansial ini juga berdampak jangka panjang pada stabilitas sistem keuangan, terutama jika kepercayaan masyarakat terhadap kemanan perbankan menurun akibat seringnya kasus *phishing*.

Dampak psikologis dan kepercayaan adalah elemen penting yang melekat dalam efek jangka pnjang dari kejahatan *phishing*. Ketika nasabah kehilangan uang, mereka tidak hanya mengalami kerugian materi, tetapi juga rasa takut dan kurang percaya terhadap sistem perbankan. Hal ini mengancam hubungan antara bank dan nasabah, yang telah dibangun atas

[77] Otoritas Jasa Keuangan, *Regulasi Ketahanan dan Keamanan Siber bagi Bank* (Jakarta: Otoritas Jasa Keuangan, 2022), 15.

dasar kepercayaan dan rasa aman. Kepercayam ini merupakan salah satu pilar utama dalam dunia perbankan, seperti yang diatur dalam Pasal 29 ayat (20 Undang-undang perbankan, yang mengharuskan bank untuk menjaga kepercayaan masyarakat melalui praktik bisnis yang sehat dan bertanggung jawab.

Ketika kepercayaan ini terganggu, kemungkinan penurunan dalam penggunaan layanan digital menjadi lebih tinggi, yang dapat memperlambat penerimaan layanan keuangan digital dan mempengaruhi pertumbuhan ekonomi digital secara keseluruhan. Oleh Karena itu, perlindungan hukum yang kuat dan transparan harus memberikan rasa aman bagi nasbah, termasuk mekanisme pengembalian yang jelas dan informasu dlam kasus kejadian kejahatan siber, seperti yang diatur dalam Undang-Undang Perlindungan Konsumen dan Undang-Undang Perlindungan Data pribadi.

Selain kerugian materi dan hilangnya kepercayaan, para korban *phishing* juga merasakan dampak psikologis seperti stress, kecemasan, trauma, dan depresi. Kekhawatiran akan hilangnya control atas data pribadi dan masalah terkait keamanan pribadi memberikan beban mentak yabng besar bagu para korban. Pengalaman ini dapat menyebabkan ketidakmampuan untuk melakukan transaksi atau menjalani aktivitas keuangan biasa, yang pada gilirannya dapat mempengaruhi kesehatan mental dan sosial korban. Dari segi hukum, perlindungan hak psikologis dan privasi korban diatur oleh Undang-Undang No. 27 Tahun 2022

tentang Perlindungan Data Pribadi, yang memberikan hak kepada korban data pribadi untuk mendapatkan perlindungan dan pemulihan data yang disalahgunakan.

Dalam kerangka hukum utama di Indonesia, peraturan yang ada yang menyediakan landasan untuk perlindungan dan penegakan terhadap kejahatan *phishing*. Salah satu undang-undang tersebuat adalah Undang-Undang Nomor 10 Tahun 1998, yang mengatur kegiatan perbankan secara umum, termasuk kewajiban bank untuk menjaga kerahasiaan dan kemanan data nasabah. Selain itu, Undang-Undang Nonmor 8 tahun 1999 tentang Perlindungan konsumen memberikan hak kepada nasabah untuk mendapatkan informasu, keamanan, dan perlindungan dari praktik yang merugikan.

C. Perlindungan Hukum Nasabah Terhadap Kejahatan *Phishing* dalam Sistem *E-banking* di Indonesia

1. Perlindungan Hukum Nasabah dalam Sistem Perbankan Digital

Transformasi menuju era digital dalam perkembangan industri telah memberikan dampak yang besar diberbagai bidang, memengaruhi Kehidupan sehari-hari. Satu sektor industri yang telah mengalami perubahan signifikan adalah sektor perbankan. Sektor perbankan mencakup berbagai hal penting, seperti aspek institusional, kegiatan usaha, serta metode dan proses yang digunakan dalam menjalankan kegiatan perbankan. Hal ini diatur dalam Pasal (1) Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Undang-Undang Nomor 7 Tahun 1992

tentang Perbankan.[78] Peraturan ini memberikan dasar hukum yang kuat bagi bank untuk menjalankan fungsinya secara efisien dan mampu beradaptasi dengan perkembangan teknologi yang pesat. Bank adalah lembaga yang didirikan berdasarkan kepercayaan. Oleh karena itu, dalam menjalankan kegiatan perbankan elektronik (*e-banking*) maupun layanan perbankan non-elektronik, bank selalu harus mematuhi peraturan yang berlaku dan menerapkan prinsip-prinsip ketelitian serta manajemen risiko.

Layanan perbankan elektronik memberikan kemudahan yang luar biasa bagi pelanggan, sehingga mereka dapat melakukan transaksi keuangan tanpa harus pergi ke cabang bank secara langsung. Hal ini sangat berguna bagi perusahaan besar yang membutuhkan sistem yang efisien, fleksibel, aman, otomatis, terintegrasi, dan andal, tanpa dibatasi oleh ruang dan waktu. Namun hingga saat ini, belum ada undang-undang yang secara khusus mengatur tentang perbankan elektronik.

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan menjadi dasar hukum dalam penerapan perbankan elektronik. Pasal 5 ayat (2) dalam undang-undang tersebut menyatakan bahwa bank komersial memiliki kewenangan untuk fokus pada kegiatan tertentu atau memberikan perhatian lebih pada sektor tertentu. Selain itu, Pasal 6 huruf (a) juga menyatakan bahwa bank komersial diperbolehkan melakukan kegiatan lain yang biasanya dilakukan oleh bank, selama tidak bertentangan dengan

[78] Sekretariat Negara Republik Indonesia, Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, Pasal 1.

peraturan perundang-undangan yang berlaku. Meskipun layanan perbankan elektronik menawarkan banyak kemudahan dan efisiensi, penerapannya tetap menghadapi tantangan, khususnya dalam aspek keamanan.[79]

Dalam dunia digital, risiko keamanan data nasabah menjadi perhatian utama, terutama karena meningkatnya jumlah kejahatan siber yang memanfaatkan celah dalam sistem perbankan. Kejahatan ini tidak hanya menyebabkan kerugian finansial, tetapi juga mengganggu integritas dan reputasi layanan perbankan. Salah satu bentuk kejahatan elektronik yang sering terjadi dalam transaksi perbankan adalah pencurian data nasabah melalui teknik *phishing*. Kejahatan *phishing* ini tidak hanya menimbulkan kerugian finansial bagi nasabah, tetapi juga mengancam kepercayaan masyarakat terhadap keamanan layanan perbankan *online* di Indonesia. Oleh karena itu, perlindungan hukum bagi nasabah sangat penting untuk memastikan keamanan dan kenyamanan dalam menggunakan layanan perbankan *online*.[80]

Phishing kasus dalam layanan *e-banking* di Indonesia semakin beragam dan sangat merugikan nasabah. Salah satu contoh nyata adalah pada 26 Agustus 2025, selebgram Jennifer Coppen menjadi korban dari sebuah penipuan *phishing* yang mempengaruhi sistem perbankan

[79] Arif Wicaksana dan Tahar Rachman, "Perlindungan Hukum bagi Pengguna Internet Banking (Mobile Banking) dari Tindakan Kejahatan Cyber," Angewandte Chemie International Edition, 6(11), 951–952. 3, no. 1 (2018): 10–27, https://medium. com/@arifwicaksanaa/pengertian-use-case-a7e576e1b6bf.

[80] Maisah dan et al, "Tinjauan Hukum Mengenai Pengamanan Data Pribadi Klien Dalam Layanan Perbankan Digital di Indonesia," Aufklarung: Jurnal Pendidikan 3, no. 3 (2023): 285–90.

elektroniknya. Kejadian ini dimulai ketika dia melakukan pembelian barang senilai hampir Rp30 juta melalui timnya, dengan pengiriman menggunakan JNE. Beberapa hari setelahnya, seorang pelaku yang menyamar sebagai JNE menghubungi tim Jennifer, mengklaim bahwa paketnya hilang dan menawarkan pengembalian dana penuh. Pelaku meminta korban untuk mengikuti prosedur pengembalian dana melalui pertemuan Zoom, kemudian mengarahkan Jennifer untuk berbagi layar, membuka aplikasi *e-banking* BCA, dan memasukkan nomor rekening virtual sebagai bagian dari proses verifikasi. Tanpa sepengetahuannya, selama proses ini, pelaku berhasil mengakses informasi sensitif dari layar korban. Akibatnya, terjadi transaksi ilegal yang mengakibatkan kehilangan Rp12.000.000 dari rekening Jennifer. Setelah mengonfirmasi dengan JNE dan bank, terungkap bahwa tidak ada prosedur resmi untuk pengembalian dana melalui Zoom atau rekening virtual, seperti yang diarahkan oleh pelaku.[81] Oleh karena itu, kejadian ini merupakan penipuan *phishing* yang menargetkan kelemahan pengguna *e-banking* melalui rekayasa sosial.

Metode ini menunjukkan berbagai ancaman *phishing* yang bisa menargetkan pelanggan. Oleh karena itu, perlindungan hukum dan tindakan pencegahan sangat penting. Bank harus memastikan sistem mereka tidak rentan terhadap serangan siber dan secara aktif mengajarkan pelanggan tentang metode terbaru. Pelanggan juga perlu meningkatkan kewaspadaan mereka, seperti tidak mengklik tautan mencurigakan, tidak

[81] Jennifer, "Pengalaman Menjadi Korban *Phishing* di E-Banking," TikTok, diunggah oleh akun @jennifer [tautan: https://vt.tiktok.com/ZSDpcCHVH/], diakses 29 September 2025.

membagikan data sensitif, serta memverifikasi keaslian aplikasi sebelum mengunduhnya. Kolaborasi antara kedua belah pihak sangat penting untuk mengatasi ancaman ini secara efektif.

Secara dasar, perlindungan yang diberikan oleh bank digital kepada pelanggannya memiliki dasar hukum yang sama dengan perlindungan konsumen seperti yang ditentukan dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Undang-Undang ini menyatakan bahwa "semua upaya untuk memastikan kepastian hukum demi memberikan perlindungan kepada konsumen" adalah wajib.[82] Oleh karena itu, bank digital secara hukum wajib melindungi hak pelanggan tanpa ada kecualian. Tahun 2021, Otoritas Jasa Keuangan (OJK) mengambil langkah-langkah untuk mendukung pengembangan *e-banking* yang aman bagi pelanggan dengan menerbitkan beberapa kebijakan penting. Salah satunya adalah Peraturan OJK Nomor 12 Tahun 2018 yang mengatur penyediaan layanan perbankan digital oleh bank komersial. Selain itu, juga ada PJOK Nomor 38 Tahun 2016 yang mengatur penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank komersial. Kebijakan-kebijakan ini bertujuan memastikan layanan perbankan elektronik yang diberikan oleh bank komersial dapat memberikan perlindungan maksimal bagi pelanggan, baik dalam hal keamanan transaksi maupun perlindungan hukum.

[82] Sekretariat Negara Republik Indonesia, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

2. Tanggung Jawab Bank terhadap Nasabah Korban *Phishing*.

Dalam upaya melindungi data pribadi pelanggan saat menggunakan layanan *e-banking* di Indonesia, terdapat berbagai hak yang dijamin kepada pelanggan. Hak-hak ini yaitu:[83]

a. Hak atas Keamanan Data Pribadi

Pelanggan berhak memastikan bahwa data pribadi yang dikumpulkan oleh bank melalui layanan perbankan digital akan dijaga keamanannya dari akses atau penggunaan yang tidak sah. Bank diwajibkan untuk menerapkan langkah-langkah keamanan yang memadai, seperti teknologi enkripsi dan otentikasi ganda, untuk melindungi data nasabah. Ketentuan ini tercantum dalam Pasal 6 dan Pasal 21 Ayat (1) Peraturan OJK No. 12/POJK. 03/2018.

b. Hak atas Informasi dan Transparansi

Pelanggan berhak mendapatkan informasi yang jelas dan lengkap mengenai pengumpulan, penggunaan, penyimpanan, dan pemrosesan data pribadi mereka oleh bank. Bank wajib memberikan penjelasan yang memadai mengenai kebijakan kerahasiaan mereka, termasuk hak pelanggan untuk memberi atau menolak persetujuan penggunaan data mereka. Ketentuan ini terdapat dalam Pasal 26 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun

[83] Ramadhanti Achlina Tri Putri dan Heru Sugiyono, "Tangguang jawab bank Terhadap Tindakan *Phishing* Dalam Sistem Penggunaan E-Banking (Studi : Kasus Phising Pada Pt . Bank Rakyat Indonesia (PERSERO) TBK)," *Jurnal Interpretasi Hukum* 4, no. 3 (2023): 682.

2016.[84]

c. Hak untuk Mengajukan Pengaduan

Jika seorang nasabah merasa bahwa hak-haknya telah dilanggar atau bahwa bank tidak menghormati kebijakan privasinya, mereka memiliki hak untuk mengajukan keluhan. Bank serta Otoritas Jasa Keuangan (OJK) menawarkan cara untuk menangani keluhan tersebut dengan cara yang adil dan terbuka. Hak ini dilindungi oleh Pasal 29 Ayat (1) dan (2) Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016.

d. Hak untuk Menghapus Data

Nasabah memiliki hak untuk meminta agar data pribadi yang tidak lagi dibutuhkan oleh bank dihapus, atau jika data tersebut digunakan dengan cara yang melanggar hukum atau kebijakan privasi. Bank diharuskan untuk menjawab permintaan ini dalam waktu yang ditetapkan oleh peraturan yang berlaku. Hak ini diatur dalam Pasal 25 Ayat (1) Huruf b dari Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016.

e. Hak untuk Mencabut Persetujuan

Pelanggan berhak untuk menarik persetujuan mengenai pemakaian data pribadi mereka. Ketika persetujuan ditarik, bank wajib untuk menghentikan penggunaan data itu kecuali terdapat kewajiban

[84] Riza Diandra Tanjung dan Nurhilmiyah, "Aspek Pelindungan Hukum Atas Data Pribadi Nasabah pada Penyelenggaraan Layanan Mobile Banking pada PT. Bank Rakyat Indonesia Cabang Stabat," *Jurnal Ilmu Hukum, Humaniora dan Politik* (JIHHP), Vol. 4, No. 5, Juli 2024, 1479, DOI: 10.38035/jihhp.v4i5.

hukum yang mengharuskan data tersebut tetap digunakan.[85]

Tujuan dari hak-hak ini adalah untuk memastikan bahwa pelanggan memperoleh perlindungan yang cukup bagi data pribadi mereka. Dengan cara ini, layanan perbankan digital dapat berfungsi dengan aman, transparan, dan memberi pelanggan lebih banyak kekuasaan atas data pribadi mereka.

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik juga memberikan kontribusi penting dalam meningkatkan keamanan dan kenyamanan bagi nasabah saat melakukan transaksi *e-banking* yang disediakan oleh bank.[86] Hal ini dapat dijelaskan melalui poin-poin berikut:

Pertama, undang-undang tersebut menegaskan bahwa bank bertanggung jawab secara hukum atas segala kerugian yang mungkin dialami nasabah akibat penggunaan layanan *e-banking*, kecuali kerugian tersebut disebabkan oleh faktor di luar kendali mereka (force majeure) atau kesalahan dari pihak nasabah.

Kedua, lembaga keuangan diwajibkan untuk memiliki sistem elektronik yang handal dan aman serta bertanggung jawab atas pengoperasiannya.

Ketiga, pengakuan terhadap kontrak elektronik berarti bahwa

[85] Tanjung dan hilmiyah, *" Aspek Perlindungan Hukum*", 1480.

[86] Sekretariat Negara Republik Indonesia, Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

laporan transaksi perbankan yang dikirim melalui email dapat dianggap sebagai suatu bentuk kontrak elektronik, yang memperkuat posisi hukum bagi nasabah.

Keempat, informasi dan dokumen elektronik diakui sebagai bukti hukum yang sah, sehingga laporan transfer rekening dalam sistem elektronik bank dapat digunakan sebagai bukti yang valid dalam transaksi perbankan.

Kelima, perundang-undangan memberikan ketentuan yang lebih jelas terkait dengan kejahatan sistem informasi, sehingga mempermudah pihak penegak hukum dalam menindak pelanggaran.

Hukum Perbankan tidak secara khusus menyebutkan perlindungan hukum untuk masyarakat yang menggunakan jasa bank. Namun, dalam Pasal 29 dari Hukum Perbankan, ada beberapa poin yang dijelaskan sebagai berikut:

a. Bank Indonesia bertanggung jawab untuk membina dan mengawasi bank-bank.
b. Bank diwajibkan untuk menjaga kesehatan bank dengan memenuhi syarat kecukupan modal, kualitas aset, kualitas manajemen, likuiditas, profitabilitas, solvabilitas, serta aspek lain yang terkait dengan operasional bank. Bank juga harus menjalankan kegiatan usaha mereka dengan prinsip kehati-hatian.
c. Ketika bank memberikan pinjaman atau pembiayaan yang sesuai dengan prinsip Syariah serta melakukan kegiatan bisnis lainnya,

penting bagi bank untuk memilih metode yang tidak merugikan baik pihaknya maupun kepentingan nasabah yang telah mempercayakan dananya kepada bank.

d. Bank diwajibkan untuk memberikan informasi kepada nasabah mengenai potensi risiko kerugian yang berkaitan dengan transaksi yang dilakukan melalui bank.[87]

Dengan demikian, Pasal 29 memberikan arahan mengenai tanggung jawab bank dalam menjaga kesehatan serta memberikan layanan yang tidak merugikan nasabah, serta kewajiban bank untuk memberikan informasi yang jelas terkait risiko transaksi kepada nasabahnya.

Namun, masih diperlukan peraturan lebih lanjut melalui regulasi pemerintah, terutama terkait dengan persyaratan minimum yang harus dipenuhi oleh sistem elektronik. Dalam hal perlindungan hukum bagi nasabah yang menjadi korban pencurian data, bank harus mengambil langkah pencegahan yang tepat, seperti memverifikasi identitas pengguna layanan perbankan dan bekerja sama dengan pihak berwenang sesuai dengan ketentuan yang berlaku tentang kerahasiaan bank.

Perlindungan bagi nasabah dapat dilaksanakan dengan dua cara: secara implisit dan eksplisit:[88]

a. Perlindungan implisit melibatkan pengawasan dan bimbingan yang efektif untuk mencegah kebangkrutan bank. Ini dapat dilakukan

[87] Asiana Granadia Dyah Buwana, *"Perlindungan Hukum Bagi Nasabah Perbankan Berdasarkan Standar Layanan di PT. Bank Negara Indonesia (Persero) Tbk"*, Reformasi Hukum, Vol. XXII No. 2, Juli–Desember 2018, 218–219.

[88] Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat Indonesia*, (Surabaya: Bina Ilmu, 1987), 20.

melalui regulasi perbankan, pengawasan oleh Bank Indonesia, menjaga kesehatan bank, dan memberikan informasi risiko kepada bank.

b. Perlindungan eksplisit mencakup pembentukan suatu lembaga yang bertanggung jawab untuk menjamin simpanan masyarakat. Jika bank mengalami masalah, lembaga tersebut akan mengembalikan uang kepada masyarakat.

Dalam konteks layanan perbankan digital, perlindungan hukum untuk nasabah Keberadaan tindak kejahatan *phishing* melalui tautan penipuan dalam sistem perbankan digital seringkali mengakibatkan kerugian finansial yang besar bagi nasabah. Oleh karena itu, perlindungan hukum bagi korban kejahatan *phishing* merupakan hal yang sangat krusial dalam sistem hukum Indonesia.

3. Upaya Perlindungan Hukum Preventif dan Represif bagi Nasabah

Perlindungan hukum bagi nasabah yang menjadi korban *phishing* dapat dibedakan menjadi dua kategori: perlindungan hukum preventif dan perlindungan hukum represif.[89]

a. Perlindungan Hukum Preventif

Perlindungan hukum preventif Adalah perlindungan yang bertujuan untuk mencegah terjadinya pelanggaran atau kerugian sebelum suatu peristiwa hukum terjadi. Dalam konteks perbankan dan kejahatan *phishing*, perlindungan hukum preventif telah diterapkan

[89] J. T. Tanonggi, I. Pusparini, C. P. Limbong, dan ..., "Tinjauan Hukum Terhadap Pertanggungjawaban Bank Kepada Data Nasabah Dalam Serangan *Phishing*," *Journal of Law*, 2024, https://jurnal.intekom.id/index.php/inlaw/article/view/504

oleh Bank Indonesia dan Otoritas Jasa Keuangan (OJK) melalui pembentukan undang-undang dan regulasi yang mengatur perlindungan konsumen dan keamanan sistem perbankan.

Otoritas Jasa Keuangan (OJK) telah memberikan perlindungan hukum preventif melalui Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Peraturan ini mengharuskan pelaku usaha jasa keuangan, termasuk bank, untuk menerapkan prinsip perlindungan konsumen, menjaga keamanan data pribadi dan dana nasabah, serta menyediakan mekanisme pengaduan dan penyelesaian sengketa.[90] Ketentuan-ketentuan ini menunjukkan bahwa OJK telah menjalankan fungsi perlindungan hukum preventifnya dengan menetapkan norma-norma yang mengikat guna mencegah kerugian nasabah akibat kejahatan digital seperti *phishing*.

Selain OJK, Bank Indonesia juga memberikan perlindungan hukum preventif melalui Peraturan Bank Indonesia Nomor 3 Tahun 2023 tentang Perlindungan Konsumen Bank Indonesia. Dalam peraturan ini, Bank Indonesia mengatur prinsip perlindungan konsumen dalam pelaksanaan sistem pembayaran, termasuk kewajiban untuk menjaga keamanan data dan dana konsumen. Perlindungan yang diberikan oleh Bank Indonesia bersifat sistematik dan pada tingkat makro, yang bertujuan untuk mencegah gangguan

[90] Otoritas Jasa Keuangan, *Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan*, Tahun 2023.

terhadap sistem pembayaran dan melindungi kepentingan konsumen secara lebih luas.[91]

Di sisi lain, bank sebagai penyedia layanan keuangan juga diwajibkan untuk melaksanakan perlindungan hukum preventif bagi nasabah mereka. Kewajiban ini diatur dalam Peraturan Otoritas Jasa Keuangan Nomor 38/POJK. 03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum. Peraturan ini mengharuskan bank untuk mengelola risiko teknologi informasi, termasuk risiko kejahatan siber dan *phishing*, dengan menerapkan sistem keamanan yang memadai serta memberikan edukasi kepada nasabah. Oleh karena itu, perlindungan hukum preventif dalam kasus *phishing e-banking* telah diterapkan oleh Bank Indonesia, OJK, dan bank melalui pembentukan regulasi dan penerapan standar keamanan.

b. Perlindungan Hukum Represif

Perlindungan hukum represif adalah Perlindungan hukum yang bersifat represif diberikan setelah terjadinya pelanggaran hukum atau kerugian bagi nasabah. Dalam konteks ini, Bank Indonesia dan Otoritas Jasa Keuangan (OJK) tidak secara langsung memberikan ganti rugi kepada nasabah yang menjadi korban *phishing*. Kedua lembaga ini berperan sebagai pengatur dan pengawas sektor perbankan, sehingga bentuk perlindungan hukum represif yang

[91] Bank Indonesia, *Peraturan Bank Indonesia Nomor 3 Tahun 2023 tentang Perlindungan Konsumen Bank Indonesia*, Tahun 2023.

diberikan dilakukan melalui penegakan regulasi dan sanksi administratif terhadap bank yang melanggar ketentuan perlindungan konsumen.[92]

Otoritas Jasa Keuangan, berdasarkan Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan, memiliki wewenang untuk menjatuhkan sanksi administratif kepada bank yang tidak memenuhi kewajiban perlindungan konsumen, mulai dari peringatan tertulis dan denda hingga pembatasan kegiatan usaha dan bahkan pencabutan izin usaha.[93] Bank Indonesia juga memiliki kewenangan untuk memberikan sanksi atas pelanggaran ketentuan sistem pembayaran sesuai dengan peraturan yang berlaku. Perlindungan hukum represif yang diterapkan oleh BI dan OJK bertujuan untuk mendorong kepatuhan dan memberikan efek jera terhadap pelanggaran yang dilakukan oleh bank.

Terkait ganti rugi atas kerugian finansial akibat kejahatan *phishing*, tanggung jawab ini ada pada pihak bank, sebagai penyedia jasa keuangan yang menyimpan dan mengelola dana nasabah. Kewajiban bank untuk menjamin keamanan dana nasabah berdasarkan prinsip fidusia, yang mendasari hubungan hukum antara bank dan nasabah. Hal ini ditegaskan dalam Pasal 29 ayat (4) Undang-Undang

[92] Maman Nurohman, Muhammad Luthfi Saputra, Shinta Putri Sanjaya, Zheea Keisha Rahmandita, dan Dikha Anugrah, "Mekanisme Perlindungan Hukum Bagi Pihak dalam Perikatan Kredit Perbankan," *LETTERLIJK: Jurnal Hukum Perdata*, Vol. 1, No. 2 (Desember 2024): 137–152.

[93] Sekretariat negara Republik Indonesia, *Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan*.

Perbankan, yang menyatakan bahwa bank wajib menjaga keamanan dana nasabah, dan Pasal 19 Undang-Undang Perlindungan Konsumen, yang mengharuskan pelaku usaha untuk memberikan ganti rugi atas kerugian yang dialami oleh konsumen.[94]

Dengan demikian, perlindungan hukum represif bagi nasabah yang menjadi korban *phishing* melalui kewajiban bank untuk menyelesaikan keluhan nasabah serta memberikan ganti rugi jika terbukti ada kelalaian dalam mengamankan sistem perbankan. Bank Indonesia dan Otoritas Jasa Keuangan berperan dalam memastikan bahwa kewajiban ini terpenuhi melalui pengawasan dan penegakan regulasi.

4. Analisis Perlindungan Hukum Nasabah Terhadap Kejahatan *Phishing* dalam Sistem *E-banking* di Indonesia

Perlindungan hukum bagi yang menjadi korban kejahatan *phishing* dalam sistem *e-banking* di Indonesia merupakan aspek penting seiring dengan transformasi digital yang cepat dalam sektor perbankan yang menghadirkan kenyamanan sekaligus resiko keamanan. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan menjadi dasar hukum utama yang mengatur lembaga perbankan, aktivitas usaha, dan proses, termasuk opedasional *e-banking* dimana bank diwajibkan untuk menajalankan fungsinya berdasarka kepercayaan dan prinsip kehati-hatian guna menjaga

[94] Jose Timothy Tanonggi, Indah Pusparini, Cantika Putri Limbong, Geby Thiffani, dan Sylvia Novelia Siagan, "Tinjauan Hukum Terhadap Pertanggungjawaban Bank Kepada Data Nasabah Dalam Serangan *Phishing*," *INLAW: Indonesian Journal of Law*, Vol. 1, No. 6 (Juni 2024): 186.

keamanan nasabah serta sistem perbankan secara keseluruhan (Pasal 1, 5, dan 6 UU 10/1998).

Layanan perbankan elektronik memberikan akses yang mudah dan transaksi yang fleksibel tanpa batasan waktu dan tempat, namun belum ada undang-undang khusus yang mengatur e-bankin. Oleh karena itu, perlindungan diterapkan sesuai dengan ketentuan perbankan umum dan peraturan terkait, seperti Peraturan OJK Nomor 12 Tahun 2018 tentang Penyediaan Layanan Perbankan Digital Oleh Bank Umum dan PJOK Nomor 38 Tahun 2016 tentang Pelaksanaan Manajemen Risiko Teknologi Informasi. Aturan ini mewajibkan bank untuk menerapkan teknologi kemanan, termasuk enskripai dan autentikasi ganda, guna melindungi data pribadi nasabah dari pencurian dan penyalahgunaan, terutama ancaman *phishing* yang dapat mengurangi kepercayaan masyarakat terhadap layanan perbankan elektronik.[95]

Kasus *phishing* yang melibatkan selebgram Jennifer Coppen pada Agustus 2025 menunjukkan bagaimana penipuan melalui rekayasa sosial dapat menipu pengguna lewat aplikasi pertemuan *online* (Zoom) dan mengendalikan akses layar, yang memungkinkan pelaku menguasai akun *e-banking* korban. Hal ini menekankan pentingnya meningkatkan sistem keamanan oleh bank dan meningkatkan kewaspadaan pelanggan saat melakukan transaksi digital.

Secara hukum, perlindungan yang diberikan oleh bank digital kepada

[95] Otoritas Jasa Keuangan, Peraturan OJK Nomor 12 Tahun 2018 tentang Penyediaan layanan perbankan Digital, (Jakarta: Otoritas Jasa Keuangan, 2018), 12.

nasabah berlandaskan pada prinsip-prinsip perlindungan konsumen yang diatur dalam Undang-Undang omor 8 Tahun 1999. Undang-undang ini mengahruskan upaya untuk memberikan kepastian hukum dan perlindungan maksimal kepada pengguna layanan, termasuk nasabah perbankan digital. Otoritas Jasa keuangan (OJK) sebagai pengawas juga telah mengeluarkan kebijakan yang mendukungg keamanan dan perlindungan hukum bagi nasabah, menekankan pentingnya manajemen risiko dalam pengguanaan teknologi informasi di bank.

Tanggung jawab bank terhadap nasabah yang menjadi korban *phishing* sangat jelas, yaitu memastikan keamanan data pribadi nasabah yang dikumpulkan dan diproses melalui layanan digital (Pasal 6 dan Pasal 21 Ayat (1) POJK No. 12/POJK. 03/2018). Nasabah juga berhak mendapatkan informasi menyeluruh mengenai kebijakan privasi bank, serta memiliki hak untuk mengajukan keluhan, menghapus data pribadi yang tidak perlu, dan mencabut persetujuan untuk penggunaan data yang telah disampaikan kepada bank (pasal-pasal terkait dalam Peraturan Menteri Komunikasi dan Informatika No. 20 tahun 2016).

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) memperkuat aspek tanggung jawab bank dengan mewajibkan mereka memiliki sistem elektronik yang dapat diandalkan dan bertanggung jawab atas operasionalnya. Undang-undang ini juga mengakui laporan transaksi elektronik sebagai bukti hukum yang sah, sehingga meningkatkan perlindungan hukum bagi nasabah dalam

transaksi perbankan digital. Pasal 29 Undang-Undang Perbankan juga mengatur kewajiban Bank Indonesia dan bank untuk menjaga kesehatan bank serta memberikan informasi yang jelas mengenai risiko kerugian yang mungkin terjadi dalam transaksi, yang merupakan bagian penting dari perlindungan nasabah.

Perlindungan hukum bagi nasabah dibagi menjadi dua pendekatan yaitu preventif dan represif.[96] Perlindungan preventif mencakup peraturan ketat seperti Peraturan Bank Indonesia No. 22/20/PBI/2020, yang mengatur standar keamanan sistem pembayaran digital, serta POJK No. 1/POJK. 07/2013, yang mewajibkan lembaga keuangan untuk memberikan edukasi kepada nasabah mengenai risiko siber, termasuk *phishing*, serta penerapan teknologi keamanan seperti otentikasi dua faktor (2FA), enkripsi, dan sistem deteksi anomali transaksi. Pendidikan literasi digital menjadi langkah penting dalam mengurangi risiko penipuan yang sering dilakukan oleh pelaku *phishing* (PBI No. 22/20 dan POJK No. 1/2013).

Perlindungan hukum yang represif merupakan tindakan yang diambil setelah terjadinya kejahatan, yang mencakup pelaporan kepada penegak hukum, penyelidikan, dan penuntutan terhadap pelaku berdasarkan Undang-Undang ITE, Kitab Undang-Undang Hukum Pidana, serta Undang-Undang Perlindungan Data Pribadi, dan juga mekanisme ganti rugi untuk korban (Pasal 19 Undang-Undang Perlindungan Konsumen dan Pasal 1365 Kitab Undang-Undang Hukum Perdata). Bank juga diwajibkan

[96] Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat Indonesia*, (Surabaya: Bina Ilmu, 1987), 20.

untuk memberikan ganti rugi jika terbukti lalai dalam menjaga sistem mereka. Namun, masih ada tantangan dalam penegakan hukum, seperti pelaku yang menggunakan teknologi canggih dan lokasi luar negeri yang menyulitkan pelacakan, serta kurangnya kesadaran pelanggan tentang keamanan data pribadi.

Dalam konteks ini, peran bank dan nasabah harus seimbang: bank perlu secara terus-menerus memperkuat sistem keamanannya dan memberikan pendidikan yang aktif, sementara nasabah diharapkan untuk meningkatkan kewaspadaan dan pemahaman mereka mengenai penipuan siber. Kerja sama yang saling mendukung ini diharapkan dapat membentuk lingkungan perbankan digital yang aman, dapat dipercaya, dan terlindungi dari serangan *phishing* yang berbahaya.

BAB V

PENUTUP

A. Kesimpulan

Berdasarkan penelitian yang telah dilakukan oleh peneliti dan disusun dalam bentuk bab demi bab, kesimpulan yang dapat diambil dari studi ini adalah sebagai berikut.:

1. Bahwa bentuk kejahatan siber yang memanfaatkan penipuan digital seperti email palsu, pesan teks, panggilan telepon, dan situs web yang tidak asli untuk mencuri data pribadi nasabah. Tindakan ini memenuhi unsur penipuan sebagaimana diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana dan melanggar ketentuan Undang-Undang ITE serta Undang-Undang Perlindungan Data Pribadi. Otoritas Jasa Keuangan (OJK) memiliki peran penting dalam mengawasi keamanan sistem perbankan digital melalui penerapan manajemen risiko teknologi informasi sesuai dengan POJK No. 38/PJOK. 03/2016. Kejahatan *phishing* tidak hanya mengakibatkan kerugian materiil tetapi juga menurunkan kepercayaan publik terhadap perbankan elektronik. Oleh karena itu, diperlukan perlindungan hukum yang ketat, peningkatan keamanan siber oleh bank, serta pendidikan digital bagi nasabah untuk mencegah dan mengurangi risiko kejahatan ini.
2. Bahwa dampak dari tindakan *phishing* terhadap pelanggan *e-banking* meliputi kehilangan finansial, berkurangnya kepercayaan, dan dampak psikologis. Banyak pelanggan kehilangan uang akibat akses yang tidak sah

ke akun mereka disebabkan oleh kebocoran data pribadi melalui situs web atau pesan palsu. Hal ini menurunkan keyakinan terhadap keamanan sistem perbankan digital dan membuat pelanggan ragu untuk memanfaatkan layanan *e-banking*. Selain itu, para korban sering mengalami stres, trauma, dan bahkan depresi akibat kehilangan kendali atas data pribadi dan dana mereka. Dari segi hukum, kejahatan ini diatur oleh Undang-Undang Informasi dan Transaksi Elektronik (ITE), Undang-Undang Perlindungan Konsumen, Undang-Undang Perlindungan Data Pribadi, dan Undang-Undang Perbankan, yang menekankan kewajiban bank untuk menjaga keamanan sistem dan memberikan perlindungan serta pemulihan kepada korban guna menumbuhkan kepercayaan dan keamanan dalam transaksi digital.

3. Bahwa untuk menjaga keamanan dan kepercayaan dalam transaksi digital. Meskipun belum ada aturan khusus yang mengatur *e-banking*, perlindungan ini diatur melalui Undang-Undang Perbankan, Undang-Undang ITE, Undang-Undang Perlindungan Konsumen, dan Undang-Undang Perlindungan Data Pribadi, serta diperkuat oleh POJK No. 12 Tahun 2018 dan POJK No. 38 Tahun 2016. Bentuk perlindungan hukum meliputi langkah-langkah pencegahan, seperti penerapan sistem keamanan (enkripsi, otentikasi ganda) dan pendidikan bagi konsumen, serta langkah-langkah represif, yaitu penegakan hukum dan kompensasi bagi para korban. Tantangan utama adalah rendahnya kesadaran publik dan kompleksitas penegakan hukum lintas batas, sehingga diperlukan sinergi

antara pemerintah, bank, dan OJK untuk membangun sistem *e-banking* yang aman dan terpercaya.

B. Saran

1. Kepada pemerintah dan pembuatan kebijakan, Pemerintah harus segera menyusun peraturan khusus yang mengatur perlindungan hukum bagi pelanggan *e-banking* dari serangan *phishing*. Peraturan ini diharapkan dapat memberikan kepastian hukum, menjelaskan tanggung jawab bank, dan memperkuat koordinasi antara Otoritas Jasa Keuangan (OJK), Bank Indonesia, serta aparat penegak hukum dalam menangani kasus kejahatan siber transnasional.
2. Kepada Otoritas Jasa Keuangan (OJK), OJK diharapkan untuk meningkatkan pengawasannya terkait penerapan manajemen risiko dan keamanan teknologi informasi di lembaga perbankan. Selain itu, OJK perlu meningkatkan literasi digital melalui edukasi publik agar pelanggan memahami risiko *phishing* dan langkah-langkah pencegahannya.
3. Kepada Lembaga Perbankan, Bank harus memperkuat sistem keamanan *e-banking* mereka dengan menerapkan teknologi enkripsi, otentikasi ganda, dan deteksi dini terhadap aktivitas mencurigakan. Bank juga sebaiknya memberikan edukasi secara rutin kepada pelanggan mengenai penipuan *phishing* dan mengambil tanggung jawab penuh jika kesalahan sistem menyebabkan kerugian.
4. Bagi nasabah diharapkan lebih berhati-hati dalam melindungi data pribadi mereka dan tidak mudah mempercayai pesan atau tautan yang mengaku

berasal dari bank. Pelanggan wajib memastikan keaslian situs atau aplikasi *e-banking* yang mereka gunakan dan segera melaporkan kepada bank dan OJK jika mereka menjadi korban *phishing*, agar penanganan dapat dilakukan dengan cepat dan tepat.

DAFTAR PUSTAKA

a. Buku

Barkatullah, Abdul Halim, *Hukum Kejahatan Siber: Tinjauan atas Cyber Crime dan Digital Evidence*. Yogyakarta: Pustaka Pelajar, 2023.

Dirdjosisworo, Soedjono, *Pengantar Ilmu Hukum*. Jakarta: RajaGrafindo Persada, 2008.

Gazali, Djuni S. , dan Rachmadi Usman, *Hukum Perbankan*. Jakarta: Sinar Grafika, 2010.

Hamzah, Andi, *Delik-Delik tertentu (Speciale Delicten) didalam KUHP edisi kedua*. Jakarta: Sinar Grafika, 2015.

Hadjon, Philipus M. , *Perlindungan Hukum bagi rakyat di Indonesia*. Surabaya: Bina Ilmu, 1987.

Hermansyah, *Hukum Perbankan Nasional Indonesia*. Jakarta: Kencana, 2011.

Ishaq, *Dasar-Dasar Ilmu Hukum*. Jakarta: Sinar Grafika, 2009.

Kasmir, *Bank dan Lembaga Keuangan Lainnya*, Edisi ke-12. Jakarta: RajaGrafindo Persada, 2012.

Kasmir, *Dasar-Dasar Perbankan*. Jakarta: RajaGrafindo Persada, 2014.

Kristiawanto, H. , *Memahami Penelitian Hukum Normatif*. Jakarta: PT Nas Media Indonesia, 2024.

Marzuki, Peter Mahmud, *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group, 2017.

Muhaimin, *Metodologi Penelitian Hukum*. Jakarta: Sinar Grafika, 2020.

Mubarok, Jaih, Fiqih Muamalah: *Konteks Doktrin dan Teori Hukum Islam*.

Otoritas Jasa Keuangan, *Regulasi Keamanan dan Ketahanan Siber untuk Bank*. Jakarta: OJK, 2022.

Purnamawati, I Gusti Ayu dkk. , *Bank dan Lembaga Keuangan Lain*. Yogyakarta: Graha Ilmu, 2014.

Rahardjo, Satjipto, *Ilmu Hukum*. Bandung: Citra Aditya Bakti, 2014.

Rahmawati, Devie, *Waspada Kejahatan Attack*. Jakarta: PT Literasi Nusantara Abadi Group, 2024.

Rasjidi, Lili, dan I. B. Wyasa Putra, *Kamus Hukum: Bahasa Indonesia dan Bahasa Inggris*. Bandung: Citra Aditya Bakti, 2015.

Rhardjo, *Budi, Keamanan Sistem Informasi Berbasis Internet*. Bandung: Informatika, 2018.

Robbins, P. , *Organizatioanl Behavior, Edisi ke-10, alih Bahasa Drs. Benyamin Molan*. Jakarta: Salemba Empat, 2003.

Romli, *Perlindungan Hukum*. Palembang: CV Doki Course and Training, 2024.

Syahdeini, Sutan Remy, *Kejahatan dan Tindak Pidana Komputer*. Jakarta: Pustaka Utama Grafika, 2009.

Vyctoria, *Bongkar Rahasia E-banking dengan Teknik Hacking dan Carding*. Yogyakarta: Penerbit Andi, 2013.

Wardhana, Aditya, *Pemanfaatan Teknologi Digital dalam berbagai Aspek Kehidupan Masyarakat.* Bandung: CV Media Sains Indonesia, 2021.

b. Jurnal

Achlina Tri Putri, Ramadhanti, dan Heru Sugiyono, "Kewajiban Bank Terhadap Kasus *Phishing* Dalam Penggunaan *E-banking* (Studi Kasus PT Bank Rakyat Indonesia (Persero) Tbk)," *Jurnal Interpretasi Hukum* 4, no. 3 (Desember 2023).

Agatha Hendarto, Vanya, dan Endang Prasetyawati, "Tanggung Jawab Bank Dalam Mencegah dan Menangani Kerugian Nasabah Karena Penipuan Melalui Link *Phishing* di Mobile Banking," Iuris Studia: *Jurnal Kajian Hukum* 5, no. 3 (Oktober 2024–Januari 2025).

Amin Muftiadi, Tri Putri Mulyani Agustina, dan Margaretha Evi, "Analisis Kasus Keamanan Jaringan Komputer: Ancaman *Phishing* Pada Layanan Internet Banking," Hexatech: *Jurnal Ilmiah Teknik* Vol. 1, No. 2 (Agustus 2022).

Clara Nervia, Kresentia Aiko Wardhana, Pricilia Angel Sie, Talitha Livia Talim, dan Waynehard Brayne Hizkia, "Studi Yuridis Mengenai Kejahatan *Phishing* Dalam Sistem Perbankan Digital Melalui Tautan Penipuan," IKON: *Jurnal Ilmu Hukum* Vol. 29, No. 2 (Agustus 2025).

Cut Mutia, "Studi Penipuan Digital Melalui Teknik *Phishing* Pada Layanan Mobile Banking," *Jurnal Transformasi Bisnis Digital* (JUTRABIDI), Vol. 1, No. 4 (Juli 2024).

Dewi Fortuna Mamonto, "Evaluasi Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Menurut Undang-Undang Nomor 27 Tahun 2022," *Jurnal Ilmiah Hukum*, Vol. X, No. X (2022).

Intania Az-zahra dan Zaky Munthaha Labib, "Perlindungan Hukum untuk Nasabah dalam Kasus *Phishing* dan Kejahatan Siber di Sektor Perbankan Indonesia," Yurisprudentia: *Jurnal Hukum Ekonomi*, Vol. 10, No. 2 (Desember 2024).

Maisah dkk. , "Analisis Hukum Mengenai Keamanan Data Pribadi Klien Dalam Layanan Perbankan Digital di Tanah Air," Aufklarung: *Jurnal Pendidikan* 3, no. 3 (2023).

Salsabila Chairunnisa, Tarsisius Murwadji, dan Nun Harrieti, "Perlindungan Hukum Bagi Nasabah Terhadap Kejahatan *Phishing* dan Hacking Dalam Layanan Bank Digital Berdasarkan Hukum Positif Indonesia," *Jurnal Hukum dan Sosial* 2, no. 1 (Februari 2024).

c. Peraturan Perundang-undangan

Undang-Undang Dasar Negara Republik Indonesia 1945.

Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.

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

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Peraturan Otoritas Jasa Keuangan Nomor 12 Tahun 2018 tentang Penyediaan Layanan Perbankan Digital.

Surat Edaran Otoritas Jasa Keuangan Nomor 21/SEOJK. 03/2017 tentang penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.

d. Skripsi

Hariyono, A. G. , Perlindungan Hukum bagi Korban *Phishing* dalam Sudut Pandang Kriminologi (Perlindungan terhadap Korban Kejahatan *Phishing* di Perspektif), Disertasi Doktor, Universitas 17 Agustus 1945 Surabaya, 2023.

Intan Selviany, "Efektivitas Pelaksanaan Undang-Undang Nomor 10 Tahun 1998 Mengenai Perbankan Terhadap Pengguna Bank Melalui Teknologi Informasi di Internet" (Skripsi, Universitas Putera Batam, 2019).

Lilis Wahyuningsih, "Dampak Ancaman *Phishing*, Kepercayaan Nasabah, dan Tingkat Keamanan Nasabah Pada Pengguna Mobile Banking di PT BRI (Persero) Tbk Cabang Jember" (Skripsi, Universitas Islam Negeri Kiai Haji Achmad Siddiq Jember, 2024).

Mayline Djuminar Silitonga, "Perlindungan Hukum Terhadap Kerugian Nasabah Bank Karena Metode *Phishing*" (Skripsi, Universitas HKBP Nommensen, 2023).

Mela Intan Yesica, "Perlindungan Hukum Bank Terhadap Nasabah Yang Menjadi Korban Metode *Phishing* Melalui PDF Palsu, Kajian Berdasarkan UU No. 10 Tahun 1998 Tentang Perbankan dan Kompilasi Hukum Ekonomi Syariah" (Skripsi, Universitas Islam Negeri Maulana Malik Ibrahim Malang, 2024).

Pangestu, R. , dan Mardijono, H. A. , "Upaya Perlindungan Hukum untuk Korban Penipuan Credit Point dalam Game Call Of Duty Mobile" (Skripsi, Universitas 17 Agustus 1945 Surabaya, 2023).

e. Website

Aji, Y. K. , dan Teukyu Muhammad Valdy Arief, "Pelaku Penipuan melalui APK di WhatsApp Ditangkap," Kompas. com, 18 Oktober 2025, https://regional.kompas.com/read/2023/10/30/183238278/pelaku-*phishing*-bermodus-apk-via-whatsapp-ditangkap-kuras-rp-14-m-tabungan

Beritasatu. com, diakses 1 Agustus 2025, https://www. beritasatu. com.

Direktorat Jenderal Perbendaharaan Kementerian Keuangan Republik Indonesia, "*Phishing*: Definisi, Tipe, dan Cara Mencegahnya," (2025), https://djppb.kemenkeu.go.id.

Infobanknews. com, "OJK Menerima 42. 257 Laporan Fraud, Total Kerugian Korban Mencapai Rp700,2 Miliar," 18 Oktober 2025, https://infobanknews.com/ojk-terima-42-257-laporan-penipuan-total-kerugian-korban-tembus-rp7002-m/

Jennifer, "Pengalaman Sebagai Korban *Phishing* di Layanan *E-banking*," TikTok, akun @jennifer, diakses 29 September 2025, https://vt.tiktok.com/ZSDpcCHVH/.

Kamus Besar Bahasa Indonesia (*Online*), diakses 1 Agustus 2025, https://kbbi.web.id/*e-banking*, https://kbbi.web.id/hukum, https://kbbi.web.id/perlindungan.

Liputan6. com, "Selain *Phishing*, Ada 9 Metode Serangan Siber yang Perlu Dikenal," (2020), https://www.liputan6.com/cek-fakta/read/5280986/tak-hanya-phising-berikut-ini-9-metode-serangan-siber-yang-perlu-diketahui.

Niagahoster. ac. id, Suryadi Kurniawan, "*Phishing*: Apa Itu, Cara Kerja, dan Solusi Menghadapinya," (2020), https://www. niagahoster.ac.id.

PT Bank Mega Syariah, diakses 1 Agustus 2025, ht tps://www.megasyariah.co.id

PERNYATAAN KEASLIAN TULISAN

Yang bertanda tangan di bawah ini :

Nama	: Sofia Widiatul Hasanah
NIM	: 214102020029
Program Stusi	: Hukum Ekonomi Syariah
Fakultas	: Syariah
Intitusi	: UIN Kiai Haji Achmad Siddiq Jember

Menyatakan dengan sebenarnya bahwa dalam hasil penelitian ini tidak terdapat unsur-unsur penjiplakan karya panelitian atau karya ilmiah yang pernah dilakukan atau dibuat orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila di kemudian hari ternyata hasil penelitian ini terbukti terdapat unsur-unsur penjiplakan dan ada klaim dari pihak lain, maka saya bersedia untuk diproses sesuai peraturan perundang-undangan yang berlaku.

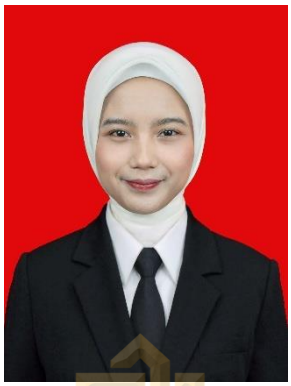
Demikian surat pernyataan ini saya buat dengan sebenarnya dan tanpa paksaan dari siapapun.

Jember, 18November 2025

Saya yang menyatakan,

SofiahWidiatul Hasanah
NIM. 214102020029

BIODATA PENULIS



Nama : Sofia Widiatul Hasana

NIM : 214102020029

TTL : Situbondo, 29 Mei 2002

Alamat : Desa Jangkar, Kec. Jangkar, Kab. Situbondo

Fakultas : Syariah

Program Studi : Hukum Ekonomi Syariah

RIWAYAT PENDIDIKAN

TK /RA : RA Nurul Bahri

SD/MI : MI Nurul Falah

SMP/MTS : SMP Ibrahimy 3 Sukorejo

SMA/MA : SMA Ibrahimy 1 Sukorejo

SARJANA : Universitas Islam Negeri Kiai Haji Achmad Siddiq Jember