Jurnal Pustaka Cendekia Hukum dan Ilmu Sosial
Volume 4, No. 1, February 2026 – May 2026, pp. 2578-2590
E-ISSN: 2987-4475
https://pchukumsosial.org/index.php/pchs

Perlindungan Hukum Bagi Nasabah Bank Akibat Phishing (Analisis Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/PID.SUS/2025/PN JKT.SEL)

Muhamad Robby Dharmawan[1], Joko Widarto[2], I Gede Hartadi Kurniawan[3]
[1, 2,3] Fakultas Hukum, Universitas Esa Unggul, Jl. Arjuna Utara No.9, RT.1/RW.2, Duri Kepa, Kec. Kb. Jeruk, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta
roby.prodharmawan@student.esaunggul.ac.id

Abstract
The development of digital banking services provides convenience and efficiency of transactions for customers, but at the same time creates legal risks in the form of phishing that harm customers. This article analyzes the legal protection of bank customers as victims of phishing and the forms of preventive efforts of banks in improving the security of digital banking services. This research adopts a normative legal analysis approach using legislative, case approaches, and conceptual. The decision analyzed is the Decision of the South Jakarta District Court Number 460/Pid.Sus/2025/PN JKT.SEL, namely the case of the distribution of phishing SMS using Fake BTS devices and the KKCSMS application. The phishing messages appeared to originate from Bank Central Asia (BCA), UOB, and HSBC, then directed customers to fake domains to enter personal and financial data such as credit card numbers, CVV, PIN, and OTP. The findings of the research suggest that legal safeguards for customers must be established through criminal law enforcement, personal data protection, consumer protection, and the principle of prudential banking. Within the framework of the Rechtsstaat, the state and financial services institutions are obliged to guarantee legal certainty, preventive protection, and effective recovery for victims. Banks are required to strengthen digital security through information technology risk management, fraud detection, customer education, monitoring of fake domains, prompt complaint handling, and coordination with regulators and law enforcement. Therefore, legal protection for phishing victims is not limited to criminal prosecution of perpetrators but must also encompass the bank's preventive obligations as a provider of digital financial services.
Keywords: Bank Customer; Digital Banking; Legal Protection; Phishing; Rechtsstaat

Abstrak
Perkembangan layanan perbankan digital memberikan kemudahan dan efisiensi transaksi bagi nasabah, tetapi pada saat yang sama menimbulkan risiko hukum berupa phishing yang merugikan nasabah. Artikel ini menganalisis perlindungan hukum terhadap nasabah bank sebagai korban phishing serta wujud upaya preventif bank dalam meningkatkan keamanan layanan perbankan digital. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, kasus, dan konseptual. Putusan yang dianalisis ialah Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL, yaitu perkara penyebaran SMS phishing menggunakan perangkat Fake BTS dan aplikasi KKCSMS. Pesan phishing tersebut seolah-olah berasal dari Bank Central Asia (BCA), UOB, dan HSBC, kemudian mengarahkan nasabah ke domain palsu untuk memasukkan data pribadi dan finansial seperti nomor kartu kredit, CVV, PIN, dan OTP. Hasil penelitian memperlihatkan bahwa perlindungan hukum terhadap nasabah harus dibangun melalui penegakan hukum pidana, pelindungan data pribadi, perlindungan konsumen, dan prinsip kehati-hatian perbankan. Dalam kerangka Rechtsstaat, negara dan lembaga jasa keuangan wajib menjamin kepastian hukum, perlindungan preventif, serta pemulihan yang efektif bagi korban. Bank wajib memperkuat keamanan digital melalui manajemen risiko teknologi informasi, deteksi fraud, edukasi nasabah, pemantauan domain palsu, penanganan pengaduan secara cepat, serta koordinasi dengan regulator dan aparat penegak hukum. Dengan demikian, perlindungan hukum bagi korban phishing tak cukup hanya melalui pemidanaan pelaku, namun juga harus mencakup kewajiban preventif bank sebagai penyelenggara layanan keuangan digital.
Kata kunci: Nasabah Bank; Perbankan Digital; Perlindungan Hukum; Phishing; Rechtsstaat.

✉Corresponding author: Muhamad Robby Dharmawan
Email Address: roby.prodharmawan@student.esaunggul.ac.id (Jl. Arjuna Utara No.9, RT.1/RW.2, Duri Kepa, Kec. Kb. Jeruk, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta)
Received 19 May 2026, Accepted 25 May 2026, Published 31 May 2026

PENDAHULUAN

Kemajuan teknologi informasi sudah mengubah pola layanan perbankan dari transaksi

konvensional menuju layanan perbankan digital, contohnya internet banking, mobile banking, kartu kredit, dan transaksi elektronik lainnya. Digitalisasi tersebut memberi kemudahan bagi nasabah karena transaksi dapat dilakukan secara cepat, praktis, dan tanpa batasan ruang. Namun, kemudahan tersebut juga menimbulkan risiko hukum baru, terutama ketika para penjahat siber memanfaatkan layanan digital untuk secara ilegal mendapatkan informasi pribadi dan finansial dari nasabah. Salah satu jenis kejahatan siber yang paling sering terjadi dalam sektor perbankan digital adalah phishing (Putra et al. 413) . Dalam dunia kejahatan siber, phishing diartikan sebagai tindakan kriminal yang memanfaatkan teknologi informasi untuk mendapatkan data atau keuntungan finansial secara ilegal (Arief 15).

Dalam layanan perbankan digital, phishing biasanya dilakukan dengan cara mengarahkan korban ke tautan yang meniru kanal resmi bank. Melalui tautan tersebut, pelaku berupaya memperoleh data sensitif nasabah, contohnya nama, nomor kartu kredit, PIN, CVV, kata sandi, dan kode OTP. Data tersebut memiliki nilai hukum dan ekonomi karena dapat digunakan untuk mengakses rekening, kartu kredit, maupun fasilitas keuangan digital lainnya (Paskaleva 106). Apabila data tersebut diperoleh melalui tautan palsu, pelaku dapat menggunakannya untuk melakukan transaksi tidak sah yang menimbulkan kerugian materiil bagi nasabah. Hal ini selaras dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menegaskan bahwa individu memiliki hak atas perlindungan informasi pribadi, termasuk saat bertransaksi secara digital.

Hubungan antara nasabah dan bank pada dasarnya dibangun atas dasar kepercayaan. Hubungan tersebut memunculkan kewajiban dan hak bagi kedua belah pihak karena bank menjalankan kegiatan usaha yang berkaitan langsung dengan dana dan kepentingan nasabah (Usman 2). Dalam layanan perbankan digital, kepercayaan tersebut tak hanya berhubungan dengan pengelolaan dana, namun juga dengan perlindungan data pribadi dan keamanan transaksi elektronik. (Herryani et al. 116).

Permasalahan tersebut terlihat di Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL. Pada kasus tersebut, terdakwa Xiang Ying bersama pihak lain diduga melakukan penyebaran SMS phishing menggunakan perangkat Fake BTS dan aplikasi KKCSMS. Pesan phishing tersebut dibuat seolah-olah berasal dari institusi keuangan ternama, yaitu Bank Central Asia (BCA), UOB, dan HSBC. Korban diarahkan untuk mengakses tautan palsu dan memasukkan data pribadi serta data kartu kredit. (Pengadilan Negeri Jakarta Selatan 6).

Perangkat Fake BTS digunakan untuk mengirimkan SMS palsu yang seolah-olah berasal dari sumber resmi dan mengarahkan korban ke tautan palsu guna memperoleh data sensitif. Modus ini menempatkan nasabah pada posisi rentan karena pesan yang diterima tampak sebagai komunikasi resmi bank. Penelitian mengenai phishing umumnya berfokus pada pemidanaan pelaku, padahal perlindungan hukum terhadap nasabah juga mencakup aspek pencegahan, penanganan, dan pemulihan kerugian. Maka dari itu, penelitian ini menganalisis perlindungan hukum terhadap nasabah bank sebagai korban phishing berdasarkan Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL dengan menggunakan teori kepastian hukum Gustav Radbruch dan teori perlindungan hukum

Satjipto Rahardjo untuk menilai kepastian norma hukum serta efektivitas perlindungan yang diberikan kepada korban.

Teori kepastian hukum Gustav Radbruch bertujuan untuk menilai sejauh mana sistem hukum memberi kejelasan norma, kepastian tanggung jawab, dan arah perlindungan bagi nasabah korban phishing (Hayoz et al. 159). Sementara itu, Teori Perlindungan Hukum Satjipto Rahardjo dijadikan landasan untuk mengkaji perlindungan hukum untuk nasabah yang mengalami kerugian akibat layanan perbankan digital (Rahardjo 53). Kedua teori tersebut digunakan untuk membaca perlindungan nasabah dalam kerangka negara hukum atau Rechtsstaat.

Berdasarkan uraian tersebut, penelitian ini merumuskan dua permasalahan utama ialah: (1) Bagaimana perlindungan hukum terhadap nasabah bank sebagai korban phishing berdasarkan Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL? dan (2) Bagaimana upaya preventif bank dalam meningkatkan keamanan layanan perbankan digital terhadap risiko phishing?

Penelitian ini tidak menempatkan bank sebagai pelaku langsung dalam tindak pidana phishing melainkan sebagai pihak yang memiliki kewajiban kehati-hatian dalam penyelenggaraan layanan perbankan digital. Maka dari itu, pembahasan diarahkan pada perlindungan hukum nasabah serta upaya preventif bank dalam memperkuat keamanan sistem, edukasi nasabah, dan mekanisme pengaduan.

METODE

Penelitian ini menerapkan metode penelitian hukum normatif (yuridis normatif), dengan menitikberatkan analisis asas, norma, serta berbagai ketentuan hukum positif yang berlaku dalam sistem hukum indonesia. Metode tersebut dipilih karena sesuai dengan tujuan penelitian, yaitu untuk menganalisis perlindungan hukum bagi nasabah bank sebagai korban phishing serta mengkaji bentuk upaya preventif bank dalam meningkatkan keamanan layanan perbankan digital berdasarkan peraturan perundang-undangan dan Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL. Metode normatif relevan digunakan karena penelitian ini berorientasi pada analisis norma hukum, interpretasi ketentuan aturan perundang-undangan, serta analisis kepada putusan pengadilan sebagai bahan kajian utama.

Penelitian ini menggunakan pendekatan perundang-undangan (statute approach), pendekatan kasus (case approach), dan pendekatan konseptual (conceptual approach). Dalam konteks perundang-undangan, penelitian ini mengkaji banyak peraturan terkait dengan perlindungan hukum nasabah, pelindungan data pribadi, perlindungan konsumen, serta penyelenggaraan teknologi informasi oleh bank, diantaranya Undang-Undang Nomor 27 Tahun 2022 terkait Pelindungan Data Pribadi, Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 terkait Penyelenggaraan Teknologi Informasi oleh Bank Umum, dan Peraturan Otoritas Jasa Keuangan Nomor 6/POJK.07/2022 terkait Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Pendekatan kasus digunakan dengan cara mengkaji Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL yang berkaitan dengan tindak pidana phishing memanfaatkan perangkat Fake BTS. Pendekatan konseptual

digunakan untuk mengkaji konsep perlindungan hukum, kepastian hukum, pelindungan data pribadi, serta kewajiban preventif bank dengan berlandaskan Teori Perlindungan Hukum yang dikemukakan oleh Satjipto Rahardjo dan Kepastian Hukum Gustav Radbruch sebagai kerangka analisis penelitian

Penelitian ini menggunakan tiga jenis sumber bahan hukum, yaitu sumber hukum primer yang meliputi undang-undang dan putusan pengadilan, sumber hukum sekunder yang mencakup jurnal, buku, dan topik penelitian terkait, dan sumber hukum tersier sebagai pelengkap. Seluruh bahan hukum diperoleh melalui studi kepustakaan (library research) kemudian dianalisis menggunakan metode kualitatif guna menghasilkan kesimpulan yang menjawab permasalahan penelitian.

HASIL DAN DISKUSI

Perlindungan Hukum terhadap Nasabah Bank sebagai Korban Phishing berdasarkan Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL

Perlindungan hukum terhadap nasabah bank sebagai korban phishing pada penelitian ini dianalisis berdasarkan Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL. Pada kasus tersebut, pelaku memanfaatkan SMS yang menyerupai komunikasi resmi bank untuk mengarahkan korban ke situs palsu. Modus tersebut menunjukkan bahwa nasabah berada pada posisi rentan karena pelaku memanfaatkan rekayasa sosial dan teknologi yang menyerupai komunikasi resmi bank (Gallo et al. 1). Kondisi tersebut menyebabkan korban sering kali tidak menyadari bahwa informasi yang diterimanya merupakan bagian dari tindak kejahatan. Perlindungan hukum tidak dapat hanya dibebankan pada kewaspadaan nasabah semata, tetapi juga memerlukan peran bank dan regulator. Penegakan hukum terhadap pelaku, kewajiban preventif bank, dan pengawasan dari regulator menjadi unsur penting dalam memberi perlindungan yang efektif bagi nasabah.

Terdapat dua jenis perlindungan hukum bagi nasabah yaitu perlindungan preventif dan perlindungan represif. Perlindungan preventif tujuannya mencegah kerugian melalui edukasi, sistem keamanan, pemantauan transaksi, dan peringatan risiko. Sementara itu, mekanisme penegakan hukum, penyelesaian pengaduan, dan pemulihan kerugian secara adil merupakan bentuk perlindungan represif (Hadjon 3; Rohendi and Kharisma 1). Kedua bentuk perlindungan tersebut saling melengkapi karena kejahatan phishing sering kali baru diketahui setelah terjadi transaksi yang merugikan korban. Nasabah membutuhkan upaya pencegahan sekaligus mekanisme pemulihan yang memadai ketika kerugian telah terjadi. Perlindungan hukum tidak terbatas pada upaya penindakan, tetapi juga pencegahan kerugian.

Penggunaan hukum pidana terhadap pelaku phishing merupakan salah satu bentuk perlindungan represif bagi nasabah. Pada putusan tersebut, terdakwa didakwa berdasarkan Undang-Undang Informasi dan Transaksi Elektronik karena membagikan informasi elektronik yang menyesatkan dan mengakibatkan kerugian materiil bagi konsumen. Dakwaan tersebut memperlihatkan bahwa phishing dipandang sebagai kejahatan yang memanfaatkan sarana elektronik dan memiliki konsekuensi hukum yang serius. Penegakan hukum pidana berfungsi memberikan kepastian hukum serta menunjukkan bahwa penyalahgunaan teknologi tidak dapat dibenarkan. Keberadaan sanksi pidana juga menjadi

sarana perlindungan bagi masyarakat dari tindak pidana yang serupa. Hal tersebut tercermin pada Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL yang menjatuhkan pidana kepada terdakwa atas penyebaran informasi elektronik menyesatkan yang membuat konsumen rugi dalam transaksi elektronik.

Walau demikian, pemidanaan kepada pelaku belum sepenuhnya memenuhi kebutuhan korban. Nasabah yang mengalami kerugian akibat transaksi tidak sah memerlukan penanganan cepat berupa pemblokiran kartu, penelusuran transaksi, dan klarifikasi terhadap transaksi yang dilakukan tanpa persetujuan. Kepastian mengenai pembagian tanggung jawab antara pihak terkait juga menjadi kebutuhan yang penting bagi korban. Apabila mekanisme tersebut tidak berjalan secara transparan, perlindungan hukum akan terasa jauh dari kebutuhan nyata nasabah. Kondisi tersebut menunjukkan bahwa pemulihan korban memiliki peranan yang sama pentingnya dengan pemidanaan pelaku (Putri Widjana et al. 451).

Perlindungan terhadap nasabah korban phishing juga berkaitan erat dengan pelindungan data pribadi. Data seperti nomor kartu kredit, CVV, PIN, dan OTP yang diperoleh melalui tautan phishing dapat digunakan untuk melakukan transaksi tidak sah. Dalam perkara yang dianalisis, korban diarahkan menuju situs palsu yang menyerupai situs resmi bank sehingga data yang dimasukkan disalahgunakan untuk pengalihan dana (Pengadilan Negeri Jakarta Selatan 16). Keadaan tersebut memperlihatkan bahwa keamanan data pribadi memiliki hubungan langsung dengan keamanan transaksi keuangan. Undang-Undang Nomor 27 Tahun 2022 terkait Pelindungan Data Pribadi memperkuat kedudukan nasabah sebagai subjek data yang berhak mendapatkan perlindungan atas data pribadinya. Fakta pada putusan tersebut memperlihatkan bahwa penyalahgunaan data pribadi ialah salah satu akibat utama dari tindak pidana phishing sehingga perlindungan data pribadi merupakan salah satu unsur penting dalam perlindungan hukum bagi nasabah yang menjadi korban phishing.

Bank memang bukan pelaku langsung dalam tindak pidana phishing, tetapi tetap memiliki kewajiban menjaga keamanan layanan yang disediakannya karena hubungan dengan nasabah didasarkan pada kepercayaan (Hermansyah). Permasalahan yang muncul bukan hanya berkaitan dengan kelalaian nasabah dalam memberikan OTP, tetapi juga mengenai kecukupan sistem pencegahan dan mekanisme pengaduan yang disediakan bank (Yuspin et al. 1699). Bank berkewajiban meningkatkan edukasi nasabah, deteksi transaksi mencurigakan, sistem autentikasi, pemantauan domain palsu, dan penanganan pengaduan (Barjaktarovic Rakocevic et al. 39). Kewajiban tersebut selaras dengan POJK Nomor 11/POJK.03/2022 terkait Penyelenggaraan Teknologi Informasi oleh Bank Umum. Implementasi prinsip kehati-hatian dalam layanan digital menjadi bagian penting dalam melindungi kepercayaan masyarakat kepada sektor perbankan.

Perlindungan konsumen menjadi dasar bagi nasabah untuk memperoleh informasi yang benar, mengakses mekanisme pengaduan, serta mendapatkan penyelesaian sengketa secara adil (Ribeiro et al. 1). Hal tersebut selaras dengan Peraturan Otoritas Jasa Keuangan Nomor 6/POJK.07/2022 terkait Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Perlindungan tersebut juga harus

dipahami dalam perspektif negara hukum yang menekankan bahwa hukum harus mampu memberi perlindungan secara nyata kepada masyarakat. Kehadiran peraturan perundang-undangan saja tidak cukup apabila tidak diikuti dengan pengawasan, penindakan, dan mekanisme pemulihan yang efektif (Anggen Suari and Sarjana 132). Dalam putusan tersebut, pelaku menggunakan identitas BCA, UOB, dan HSBC untuk memperoleh kepercayaan korban sehingga kesalahan tidak dapat sepenuhnya dibebankan kepada nasabah. Perlindungan hukum terhadap korban phishing pada akhirnya harus diarahkan tidak hanya pada penindakan pelaku, namun juga pada penguatan peran bank dan regulator dalam mencegah terulangnya risiko yang sama. Dengan demikian, putusan tersebut memperlihatkan bahwa perlindungan hukum terhadap nasabah korban phishing diwujudkan melalui penegakan hukum pidana kepada pelaku, pengakuan terhadap kerugian yang dihadapi korban sebagai konsumen transaksi elektronik, serta penguatan perlindungan data pribadi dalam layanan perbankan digital. Putusan tersebut juga menegaskan pentingnya sinergi antara bank, regulator, dan aparat penegak hukum dalam memberi perlindungan hukum yang efektif kepada nasabah.

Upaya Preventif Bank sebagai Bentuk Perlindungan Hukum terhadap Nasabah Korban Phishing

Upaya preventif bank merupakan bagian penting dari perlindungan nasabah karena phishing sering terjadi sebelum korban menyadari adanya kejahatan. Serangan phishing umumnya dilakukan melalui komunikasi palsu yang menyerupai komunikasi resmi bank sehingga pencegahan tidak cukup hanya dengan memperkuat sistem internal. Bank juga perlu memastikan bahwa nasabah dapat membedakan kanal resmi dan kanal palsu dengan mudah. Pencegahan yang efektif akan mengurangi kemungkinan nasabah terjebak pada tautan palsu. Kondisi tersebut menunjukkan bahwa perlindungan terhadap nasabah memerlukan peran aktif bank dalam membangun keamanan layanan digital (Yuspin et al. 1704).

Serangan phishing memanfaatkan kelemahan pengetahuan nasabah dan teknik rekayasa sosial yang menyerupai komunikasi resmi bank. Meskipun bank bukan pelaku langsung dalam tindak pidana phishing, bank tetap memiliki kewajiban kehati-hatian sebagai penyelenggara layanan perbankan digital. Kewajiban tersebut meliputi penguatan sistem keamanan, edukasi nasabah, serta penyediaan mekanisme pengaduan yang cepat dan efektif. Langkah preventif pertama yang perlu dilakukan adalah memperkuat sistem keamanan dan manajemen risiko teknologi informasi. Bank perlu menerapkan autentikasi berlapis, pemantauan transaksi secara real time, deteksi anomali, pembatasan transaksi berisiko, serta peringatan dini terhadap aktivitas yang menyimpang dari pola transaksi nasabah (Rohendi and Kharisma 3). Upaya tersebut selaras dengan POJK Nomor 11/POJK.03/2022 yang menempatkan keamanan teknologi informasi sebagai bagian dari tata kelola dan manajemen risiko bank.

Edukasi nasabah juga merupakan bagian penting dalam pencegahan phishing. Pelaku umumnya menggunakan pesan yang mendesak dan tampilan yang meyakinkan untuk memperoleh kepercayaan korban. Pada Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL, pesan

palsu dibuat seolah-olah berasal dari BCA, UOB, dan HSBC dengan narasi mengenai poin atau reward yang akan kedaluwarsa (Pengadilan Negeri Jakarta Selatan 10). Modus tersebut menunjukkan bahwa pelaku memanfaatkan rasa percaya dan kekhawatiran korban. Karena itu, bank perlu terus mengedukasi nasabah agar tidak memberikan data sensitif kepada siapa pun yang mengatasnamakan bank.

Pemantauan domain palsu juga menjadi langkah preventif yang penting. Dalam perkara yang dianalisis, pelaku menggunakan domain yang menyerupai identitas BCA, seperti bca.onl, bca.monster, bca-co.cyou, dan bca-co.biz. Kemiripan domain tersebut dapat menimbulkan kesan bahwa situs tersebut merupakan situs resmi bank. Bank perlu melakukan pemantauan terhadap penyalahgunaan merek dan domain serta berkoordinasi untuk melakukan pemblokiran terhadap situs palsu. Tindakan cepat diperlukan agar jumlah korban tidak semakin bertambah.

Kanal pengaduan yang responsif juga perlu diperkuat karena transaksi tidak sah dapat terjadi dalam waktu singkat setelah korban memasukkan data pada tautan palsu. Bank perlu menyediakan layanan pengaduan yang dapat diakses melalui berbagai sarana dan segera melakukan langkah pengamanan setelah menerima laporan. Pemblokiran kartu, pembatasan transaksi, penelusuran transaksi, serta pemberian informasi mengenai perkembangan penanganan menjadi bagian penting dalam proses tersebut. Mekanisme yang lambat justru dapat memperbesar kerugian dan menurunkan kepercayaan masyarakat terhadap layanan digital. Hal tersebut menunjukkan pentingnya pelayanan yang cepat dan transparan bagi korban phishing (Hendarto and Prasetyawati 764).

Pencegahan phishing juga membutuhkan kerja sama lintas lembaga karena kejahatan ini tidak selalu berasal dari sistem internal bank. Dalam perkara yang dikaji, penyelidikan dilakukan bersama KOMDIGI dengan menggunakan spectrum analyzer, BTS hunter, dan aplikasi G-NET untuk mendeteksi BTS ilegal. Fakta tersebut menunjukkan bahwa penanggulangan phishing memerlukan keterlibatan berbagai pihak. Kerja sama antara bank, OJK, Bank Indonesia, Kementerian Komunikasi dan Digital, penyelenggara telekomunikasi, dan aparat penegak hukum diperlukan agar pencegahan dapat berjalan secara terpadu. Selain itu, desain komunikasi resmi bank juga perlu dibuat konsisten dan mudah diverifikasi oleh nasabah. Bank dapat menyediakan daftar domain resmi dan kanal pelaporan pesan mencurigakan agar penyalahgunaan identitas bank dapat segera diketahui.

Perlindungan data pribadi dan keamanan transaksi harus menjadi bagian dari rancangan layanan sejak awal. Bank juga perlu mengimplementasikan konsep privacy by design dalam pelayanan digital. Pembatasan data yang diminta, enkripsi data sensitif, audit keamanan, dan pengawasan terhadap pihak ketiga merupakan langkah yang penting untuk dilakukan. Prinsip tersebut diperlukan karena serangan phishing sering memanfaatkan celah antara sistem, komunikasi digital, dan perilaku pengguna. Dengan rancangan keamanan yang baik, risiko penyalahgunaan data dapat ditekan sebelum menimbulkan kerugian yang lebih besar (Vania et al. 654).

Upaya preventif bank bukan merupakan tindakan sukarela, melainkan kewajiban yang melekat pada penyelenggaraan layanan perbankan digital. Digitalisasi memang memberikan manfaat bagi bank, tetapi pada saat yang sama juga menghadirkan risiko yang harus dikelola secara bertanggung jawab.

Seluruh risiko phishing tidak dapat dibebankan kepada nasabah karena bank memiliki sumber daya, teknologi, dan pengetahuan yang lebih memadai. Dalam kerangka Rechtsstaat, negara juga harus menjamin adanya standar keamanan sistem elektronik, mekanisme pengaduan, dan pembagian tanggung jawab yang jelas. Pengawasan OJK terhadap kesiapan teknologi informasi dan efektivitas edukasi nasabah menjadi penting untuk mewujudkan perlindungan konsumen dan kepastian hukum dalam layanan perbankan digital (Putri Widjana et al. 452).

Studi Kasus

Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL digunakan sebagai studi kasus karena menggambarkan tindak pidana phishing. Kasus ini mengikutsertakan terdakwa Xiang Ying, warga negara Tiongkok, yang didakwa bersama pihak lain, termasuk Ye Xingchi yang penuntutannya dilakukan secara terpisah. Dalam dakwaan juga disebutkan beberapa nama lain, antara lain Xiang Lei, Gaga Meng, Nancy, dan Jin Gang Ciu. Perkara tersebut termasuk perkara Informasi dan Transaksi Elektronik karena penyebaran pesan dilakukan melalui sarana elektronik. Dari awal, perkara ini memperlihatkan bahwa phishing dapat dijalankan oleh jaringan lintas orang, lintas perangkat, dan lintas lokasi.

Kasus Posisi

Berdasarkan fakta persidangan, Terdakwa Xiang Ying direkrut oleh Xiang Lei dan datang ke Indonesia untuk mengoperasikan perangkat Fake BTS yang dipasang pada kendaraan Toyota Avanza. Atas instruksi melalui Telegram, terdakwa menyebarkan SMS phishing di berbagai lokasi di Jakarta dan sekitarnya dengan mengatasnamakan BCA, UOB, dan HSBC. Pesan tersebut berisi pemberitahuan bahwa poin atau reward nasabah akan kedaluwarsa dan mengarahkan korban ke tautan tertentu untuk memasukkan data pribadi dan finansial. Modus tersebut menunjukkan penyalahgunaan identitas bank melalui pesan dan tautan yang menyerupai situs resmi. BCA menegaskan bahwa pesan tersebut bukan berasal dari pihaknya dan tidak terdapat program penukaran poin sebagaimana dicantumkan dalam SMS phishing. Dari hasil penelusuran diketahui bahwa SMS phishing diterima oleh 259 nasabah dan 55 orang di antaranya mengakses tautan palsu. Kerugian yang ditimbulkan mencapai sekitar Rp888.854.497 dengan beberapa korban yang disebutkan dalam perkara, antara lain Dina Islami, Kristo Molina, Rico Kastilani, Digga Febriawan Putra, dan Handri Winata.

Pertimbangan Hakim

Dalam memeriksa perkara Nomor 460/Pid.Sus/2025/PN JKT.SEL, Majelis Hakim mendasarkan pertimbangannya pada keterangan ahli, keterangan terdakwa, keterangan saksi, barang bukti, dan alat bukti elektronik. Menurut fakta persidangan, Majelis Hakim menemukan bahwa Terdakwa Xiang Ying bersama pihak lain mengoperasikan perangkat Fake BTS untuk menyebarkan SMS phishing yang mengatasnamakan BCA, UOB, dan HSBC. SMS tersebut berisi informasi menyesatkan mengenai penukaran poin hadiah dan mengarahkan korban ke situs palsu untuk memperoleh data pribadi dan data

finansial yang kemudian digunakan untuk melakukan transaksi tanpa persetujuan pemilik rekening sehingga menimbulkan kerugian materiil bagi korban.

Majelis Hakim juga mempertimbangkan keterangan ahli yang menjelaskan bahwa perangkat Fake BTS bekerja dengan memancarkan sinyal palsu yang lebih kuat daripada sinyal operator resmi sehingga telepon seluler korban secara otomatis terhubung dengan perangkat tersebut. Ahli juga menerangkan bahwa aplikasi KKCSMS digunakan untuk mengendalikan penyebaran SMS phishing melalui sistem yang terintegrasi. Keterangan ahli digital forensik menunjukkan adanya keterkaitan antarpelaku melalui server pengendali, struktur kode, dan fungsi operasional yang identik. Fakta tersebut menunjukkan bahwa terdakwa melakukan perbuatannya bersama pihak lain dalam suatu jaringan yang terorganisasi. Keseluruhan alat bukti tersebut memperkuat keikutsertaan terdakwa atas tindak pidana yang didakwakan.

Berdasarkan seluruh alat bukti yang diajukan di persidangan, Majelis Hakim berpendapat bahwa perbuatan terdakwa telah memenuhi seluruh unsur Pasal 45A ayat (1) Jo. Pasal 28 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Jo. Pasal 55 ayat (1) ke-1 KUHP Jo. Pasal 46 KUHP. Majelis Hakim menyatakan bahwa terdakwa dengan sengaja mendistribusikan dan/atau mentransmisikan informasi elektronik yang memuat pemberitahuan bohong atau informasi menyesatkan sehingga menyebabkan kerugian materiil bagi konsumen dalam transaksi elektronik. Oleh karena seluruh unsur tindak pidana telah terbukti, Terdakwa dinyatakan terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana sebagaimana didakwakan. Atas dasar itu, Majelis Hakim menjatuhkan pidana penjara selama 5 tahun dan pidana denda sejumlah Rp500.000.000 subsidair 6 bulan kurungan.

Amar Putusan

Dari fakta-fakta yang terbukti pada persidangan tersebut, Majelis Hakim Pengadilan Negeri Jakarta Selatan kemudian menjatuhkan putusan kepada terdakwa Xiang Ying. Dalam amar Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL, Majelis Hakim menyatakan Terdakwa Xiang Ying telah terbukti dengan sah dan meyakinkan bersalah menjalankan tindak pidana membagikan informasi elektronik yang menyesatkan dan membuat konsumen rugi dalam transaksi elektronik. Atas perbuatannya, terdakwa dijatuhi pidana penjara selama 5 (lima) tahun dan pidana denda sejumlah Rp500.000.000,00 dengan ketentuan jika denda tersebut tidak dibayar maka diganti dengan pidana kurungan selama 6 (enam) bulan. Di samping itu, Majelis Hakim menetapkan terdakwa tetap berada dalam tahanan, menentukan status barang bukti, serta membebankan biaya perkara kepada terdakwa.

Analisis Putusan

Berdasarkan pertimbangan Majelis Hakim dalam Putusan Nomor 460/Pid.Sus/2025/PN JKT.SEL, terdakwa terbukti turut serta mengoperasikan perangkat Fake BTS dan aplikasi KKCSMS untuk menyebarkan SMS phishing yang mengatasnamakan BCA, UOB, dan HSBC. Perbuatan tersebut

dilakukan dengan tujuan memperoleh data pribadi dan data finansial korban sehingga membuat kerugian materiil bagi pelanggan dalam transaksi elektronik.

Majelis Hakim juga mempertimbangkan bahwa penggunaan perangkat Fake BTS memungkinkan pengiriman SMS yang seolah-olah berasal dari institusi resmi sehingga menyesatkan korban untuk mengakses tautan palsu dan memasukkan data pribadi, CVV, PIN, serta OTP. Fakta tersebut menjadi dasar terpenuhinya unsur penyebaran informasi elektronik yang menyesatkan dan merugikan konsumen dalam transaksi elektronik.

Ditinjau dari Teori Kepastian Hukum Gustav Radbruch, putusan ini telah memberikan kepastian hukum terhadap pelaku tindak pidana phishing. Majelis Hakim telah menerapkan ketentuan hukum yang berlaku berdasarkan fakta-fakta yang terbukti dalam persidangan sehingga terdakwa mampu dimintai pertanggungjawaban atas perbuatannya. Putusan itu menunjukan bahwa setiap individu yang melakukan pelanggaran hukum dengan media elektronik tetap dapat dikenai tuntutan dan dijatuhi sanksi sesuai peraturan hukum yang ada. Berdasarkan kesaksian, proses persidangan, pendapat ahli, serta bukti-bukti yang menunjukkan keterlibatan terdakwa turut serta dalam pengoperasian perangkat Fake BTS dan penggunaan aplikasi KKCSMS untuk menyebarkan SMS phishing. Fakta tersebut membuktikan adanya penyebaran informasi elektronik yang menyesatkan sehingga penerapan Pasal 45A ayat (1) jo. Pasal 28 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik sudah sesuai dengan fakta hukum yang terbukti di persidangan.

Selain itu, Ditinjau dari Teori Perlindungan Hukum Satjipto Rahardjo, putusan tersebut mencerminkan pelaksanaan perlindungan hukum represif oleh negara sebagai respons terhadap terjadinya pelanggaran hukum. Penjatuhan pidana kepada terdakwa menunjukkan bahwa negara memberikan perlindungan kepada masyarakat, khususnya nasabah bank yang menjadi korban phishing. Putusan tersebut juga diinginkan mampu memberi efek jera bagi para pelaku dan mendorong pencegahan kejahatan serupa di waktu yang akan datang.

Meskipun demikian, perlindungan hukum terhadap nasabah tidak hanya dilakukan melalui pemidanaan pelaku. Perlindungan tersebut juga perlu didukung dengan upaya pencegahan, seperti peningkatan keamanan sistem perbankan digital, edukasi kepada nasabah mengenai modus phishing, serta penguatan perlindungan data pribadi. Dengan terdapatnya upaya represif dan preventif secara bersamaan, perlindungan hukum bagi nasabah mampu terlaksana secara lebih optimal.

Selain aspek pertanggungjawaban pidana dan perlindungan hukum terhadap korban, putusan ini juga memiliki nilai penting dari sisi pembuktian karena menguraikan secara rinci modus operandi serta teknologi yang digunakan dalam tindak pidana phishing.

Dari sisi pembuktian teknis, perkara ini penting karena menguraikan cara kerja Fake BTS dan aplikasi KKCSMS. Ahli menjelaskan bahwa Fake BTS bekerja menyerupai pemancar sinyal seluler yang dapat mengganggu sinyal operator asli. Setelah sinyal asli terganggu, perangkat tersebut memancarkan sinyal palsu yang lebih kuat sehingga ponsel korban dapat terhubung tanpa

sepengetahuan korban. Aplikasi KKCSMS digunakan sebagai perangkat lunak kendali dalam sistem penyebaran SMS phishing berbasis Fake BTS. Uraian teknis ini memperlihatkan bahwa phishing dalam perkara tersebut tidak hanya bergantung pada tipu daya, namun juga pada penggunaan perangkat teknologi yang dapat memanipulasi saluran komunikasi korban.

Analisis terhadap putusan tersebut menunjukkan bahwa perlindungan terhadap nasabah harus bergerak pada dua jalur. Jalur pertama adalah penindakan terhadap pelaku yang menyebarkan informasi bohong, menggunakan sarana elektronik secara melawan hukum, dan menyebabkan kerugian konsumen. Jalur kedua adalah perbaikan tata kelola pencegahan agar modus yang sama tidak terus berulang. Apabila perkara semacam ini hanya dilihat sebagai keberhasilan menangkap pelaku, maka persoalan yang lebih mendasar mengenai keamanan layanan digital dapat terabaikan. Putusan ini karena itu perlu dibaca sebagai bahan evaluasi terhadap kesiapan hukum, bank, dan regulator dalam menghadapi kejahatan perbankan digital.

Putusan ini juga memperlihatkan bahwa perlindungan konsumen digital tak mampu dilepaskan dari gagasan Rechtsstaat. Dalam negara hukum, nasabah tidak boleh dibiarkan menghadapi kejahatan digital seorang diri, terlebih ketika kejahatan tersebut menggunakan perangkat yang sulit dikenali masyarakat umum. Negara, regulator, bank, aparat penegak hukum, dan penyelenggara telekomunikasi harus membangun perlindungan yang saling terhubung. Penegakan hukum terhadap pelaku perlu disertai pencegahan, edukasi, dan mekanisme pemulihan bagi korban. Dengan cara demikian, putusan ini tak hanya menjadi catatan perkara pidana, namun juga cermin bagi perlindungan terhadap nasabah dalam layanan perbankan digital.

KESIMPULAN

Perlindungan hukum bagi nasabah bank yang menjadi korban phishing tidak terbatas pada penuntutan pidana terhadap pelaku, tetapi juga mencakup perlindungan data pribadi, perlindungan konsumen, serta pelaksanaan prinsip kehati-hatian oleh bank. Berdasarkan Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL, terdakwa Xiang Ying terbukti melakukan tindak pidana penyebaran informasi elektronik yang menyesatkan dan membuat konsumen rugi dalam transaksi elektronik. Putusan tersebut memperlihatkan adanya perlindungan hukum represif melalui pemidanaan pelaku, sekaligus memberikan kepastian hukum bagi masyarakat. Dalam perspektif Teori Kepastian Hukum Gustav Radbruch dan Teori Perlindungan Hukum Satjipto Rahardjo, perlindungan terhadap nasabah korban phishing harus menjamin kepastian hukum, keamanan data pribadi, serta perlindungan hukum yang efektif bagi nasabah korban phishing.

Upaya preventif bank dalam meningkatkan keamanan layanan perbankan digital merupakan bagian dari kewajiban kehati-hatian yang melekat pada penyelenggaraan layanan perbankan digital. Bank tidak dapat diposisikan sebagai pelaku langsung dalam tindak pidana phishing, namun tetap memiliki kewajiban untuk memperkuat sistem keamanan teknologi informasi, meningkatkan edukasi kepada nasabah, melakukan pemantauan terhadap domain palsu yang mengatasnamakan bank,

menyediakan mekanisme pengaduan yang cepat dan efektif, serta memperkuat kerja sama dengan regulator dan aparat penegak hukum. Upaya tersebut diperlukan untuk mencegah terjadinya kerugian yang lebih tinggi sekaligus memperkuat kepercayaan masyarakat terhadap layanan perbankan digital.

Bank sebagai penyelenggara layanan perbankan digital perlu terus meningkatkan perlindungan terhadap nasabah melalui penguatan sistem keamanan teknologi informasi, penerapan autentikasi berlapis, peningkatan sistem deteksi transaksi mencurigakan, serta edukasi yang berkelanjutan mengenai modus-modus phishing yang berkembang. Selain itu, bank perlu memperkuat mekanisme penanganan pengaduan dan pemulihan kerugian agar nasabah memperoleh perlindungan hukum yang lebih efektif ketika menjadi korban kejahatan siber.

Otoritas Jasa Keuangan, Bank Indonesia, Kementerian Komunikasi dan Digital, penyelenggara telekomunikasi, serta aparat penegak hukum butuh memperkuat koordinasi dan pengawasan kepada perkembangan kejahatan phishing dalam sektor perbankan digital. Pengawasan terhadap penyalahgunaan teknologi seperti Fake BTS, peningkatan literasi keamanan digital masyarakat, dan penguatan lebih lanjut tentang perlindungan data pribadi serta perlindungan konsumen jasa keuangan, perlu terus dilakukan guna menciptakan sistem perbankan digital yang aman dan dapat diandalkan, yang memberi kepastian hukum kepada masyarakat.

REFERENSI

Arief, Barda Nawawi. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia*. Edisi 1, Raja Grafindo Persada, 2006.

Hadjon, Philipus M. *Perlindungan Hukum Bagi Rakyat Indonesia: Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum Dan Pembentukan Peradilan Administrasi Negara*. Bina Ilmu, 1987.

Hermansyah. *Hukum Perbankan Nasional Indonesia*. Edisi 3, Prenada Media, 2020.

Rahardjo, Satjipto. *Ilmu Hukum*. Cetakan 8, Citra Aditya Bakti, 2014.

Usman, Rachmadi. *Aspek-Aspek Hukum Perbankan Di Indonesia*. Cetakan 1, Gramedia Pustaka, 2001.

Anggen Suari, Kadek Rima, and I. Made Sarjana. "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia." *Jurnal Analisis Hukum*, vol. 6, no. 1, Apr. 2023, pp. 132–42, https://doi.org/10.38043/jah.v6i1.4484.

Barjaktarovic Rakocevic, Sladjana, et al. "An Interplay Between Digital Banking Services, Perceived Risks, Customers' Expectations, and Customers' Satisfaction." *Risks*, vol. 13, no. 3, Feb. 2025, p. 39, https://doi.org/10.3390/risks13030039.

Gallo, Luigi, et al. "The Human Factor in Phishing: Collecting and Analyzing User Behavior When Reading Emails." *Computers and Security*, vol. 139, Apr. 2024, https://doi.org/10.1016/j.cose.2023.103671.

Hayoz, Nicolas, et al. "Rule of Law and Rechtsstaat under Pressure: Introductory Considerations." *Zeitschrift Fur Vergleichende Politikwissenschaft*, vol. 19, no. 2, Jun. 2025, pp. 159–74, https://doi.org/10.1007/s12286-025-00648-9.

Hendarto, Vanya Agatha, and Endang Prasetyawati. "Tanggung Jawab Bank Dalam Mengantisipasi Dan Menangani KerugianNasabah Akibat Scam Melalui Link Phising Pada Mobile Banking." *IURIS STUDIA: Jurnal Kajian Hukum*, vol. 5, no. 4, Mar. 2024, pp. 759–10765, https://doi.org/10.61132/jutrabidi.v1i4.191.

Herryani, Mas Rara Tri Retno, et al. "Legal Liability for Personal Data Misuse in Digital Banking." *Hang Tuah Law Journal*, Apr. 2026, pp. 116–34, https://doi.org/10.30649/htlj.v10i1.361.

Paskaleva, Mariya. "The Economic Value of Personal Data In Digital Economy." *International Journal of Economic Practice and Policy*, vol. 21, no. 2, 2024, pp. 106–18, https://doi.org/10.5937/skolbiz2-54701.

Putra, Fauzan Prasetyo Eka, et al. "Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study." *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, Aug. 2024, pp. 413–21, https://doi.org/10.47709/brilliance.v4i1.4357.

Putri Widjana, Ni Putu J. M., et al. "Pertanggungjawaban Bank Terhadap Kerugian Nasabah Akibat Pencurian Dana Melalui Phising." *Lokus: Jurnal Konsep Ilmu Hukum*, vol. 5, no. 3, 2025, https://doi.org/10.56128/jkih.v5i3.649.

Ribeiro, Liliana, et al. "Which Factors Predict Susceptibility to Phishing? An Empirical Study." *Computers & Security*, vol. 136, Jan. 2024, p. 103558, https://doi.org/10.1016/j.cose.2023.103558.

Rohendi, Acep, and Dona Budi Kharisma. "Personal Data Protection in Fintech: A Case Study from Indonesia." *Journal of Infrastructure, Policy and Development*, vol. 8, no. 7, 2024, https://doi.org/10.24294/jipd.v8i7.4158.

Vania, Cindy, et al. "Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber." *Jurnal Multidisiplin Indonesia*, vol. 2, no. 3, Mar. 2023, pp. 654–66, https://doi.org/10.58344/jmi.v2i3.157.

Yuspin, Wardah, et al. "Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities." *International Journal of Safety and Security Engineering*, vol. 14, no. 6, Dec. 2024, pp. 1699–706, https://doi.org/10.18280/ijsse.140605.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.

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

Putusan Pengadilan Negeri Jakarta Selatan Nomor 460/Pid.Sus/2025/PN JKT.SEL.