J-CEKI : Jurnal Cendekia Ilmiah
Vol.5, No.1, Desember 2025

Perlindungan Hukum Korban *Cyber Crime Phising* Data Nasabah Bank Dihubungkan Dengan Undang-Undang No 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik

Tomi Agi Fratama
Fakultas Hukum Universitas Nusa Cendana, Indonesia
E-mail: tomi.fratama@staf.undana.ac.id

Article History:
Received: 11 November 2025
Revised: 01 Desember 2025
Accepted: 11 Desember 2025

Keywords: Phishing Perbankan Digital; Hukum Perlindungan Data Pribadi Indonesia; Cybercrime Perbankan

Abstract: *Perkembangan digital banking secara cepat meningkatkan eskalasi risiko cybercrime dalam transaksi keuangan daring. Tujuan penelitian mengkaji perlindungan hukum nasabah bank pada kasus phishing dalam kerangka hukum Indonesia untuk membangun doktrin komprehensif terkait pertanggungjawaban hukum pada tata kelola keuangan digital. Penelitian menggunakan desain kepustakaan dengan pendekatan peraturan perundang-undangan serta interpretasi kualitatif dalam menelaah norma hukum pada struktur hukum positif nasional. Temuan penelitian menegaskan kedudukan data pribadi sebagai objek hukum terlindungi berdasarkan rezim regulasi eksplisit dalam infrastruktur keuangan digital. Diskursus empiris mengidentifikasi kewajiban sentral lembaga perbankan menjaga keamanan data sepanjang siklus pemrosesan data pribadi berlandaskan tujuan sah, kontrol keamanan, akuntabilitas risiko, serta pertanggungjawaban dapat ditegakkan. Tata kelola hukum dan kewajiban kepatuhan formal membentuk kewajiban pencegahan terhadap akses tanpa kewenangan dan manipulasi informasi elektronik. Arah penelitian lanjutan diarahkan pada pengembangan model hukum komparatif untuk standarisasi operasional penegakan keamanan data pribadi lintas sistem hukum.*

PENDAHULUAN

Perkembangan teknologi informasi pada sektor perbankan memfasilitasi pelaksanaan transaksi keuangan secara cepat, efisien, dan masif. Perkembangan digital perbankan turut membawa ancaman kejahatan siber seperti phishing sebagai risiko serius bagi keamanan finansial publik modern. Phishing dipahami sebagai tindakan penipuan melalui strategi manipulasi psikologis untuk memperoleh data pribadi nasabah berupa nomor rekening, username, password, atau PIN dengan tujuan akses ilegal terhadap akun keuangan. Teknologi informasi dipahami sebagai aktivitas mengumpulkan, mengorganisasi, menyimpan, menerbitkan, serta memanfaatkan data dalam format visual, grafik, teks, angka, audio, atau video berbasis sistem multimedia terintegrasi berbantuan perangkat komputer dan telekomunikasi (Lendo, 2025).

Adopsi layanan e-banking yang berkembang cepat memicu intensitas ancaman kejahatan siber sektor finansial yang berdampak langsung pada nasabah perbankan dalam skala luas. Phishing didefinisikan sebagai bentuk kejahatan digital berbasis rekayasa sosial tingkat tinggi karena pelaku menyamar sebagai lembaga terpercaya melalui email palsu, pesan singkat, aplikasi percakapan digital, atau website tiruan untuk memancing pemilik akun menyerahkan data sensitif seperti username, password, nomor kartu kredit, atau OTP. Phisher menyiapkan konten digital palsu yang dibuat menyerupai sistem formal perbankan sehingga korban terjebak dalam validitas palsu komunikasi elektronik (Banjarnahor & Priyana, 2022).

Serangan phishing pada sektor perbankan di Indonesia semakin bertambah sejalan dengan rendahnya tingkat literasi keamanan digital masyarakat serta kurang optimalnya pengamanan data pribadi, sehingga perlu kejelasan kerangka hukum dalam proses pencegahan maupun penindakannya. Phishing serta pembajakan privacy secure termasuk kategori cyber crime yang berfokus pada pencurian data pribadi maupun akses ilegal terhadap sistem perbankan (Amru et al., 2025). Kejahatan tersebut termasuk high-tech crime yang menimbulkan kerugian besar bagi nasabah karena tidak hanya menargetkan aset finansial, tetapi juga identitas digital korban (Budhihartanti, 2020). Tindak pidana cyber crime phishing wajib diposisikan sebagai kejahatan serius yang berdampak luas, sehingga regulasi perbankan dan Undang-Undang ITE wajib diperkuat untuk memberikan jaminan perlindungan hukum yang proporsional kepada nasabah.

Skema phishing mengeksploitasi kelemahan psikologis dan keterbatasan pemahaman teknis pengguna layanan perbankan digital. Korban sering diarahkan untuk menekan tautan berbahaya atau memasukkan kredensial pada situs palsu melalui berbagai dalih, termasuk pembaruan sistem, verifikasi akun, penawaran hadiah bernilai, atau peringatan keamanan palsu yang sengaja dirancang untuk mencuri kredensial keamanan korban. Keberhasilan phishing tidak hanya bertumpu pada kecanggihan teknis phisher dalam meniru entitas sah tetapi juga sangat bergantung pada kelalaian korban atau kurangnya uji tuntas dalam memvalidasi keaslian komunikasi atau tautan yang diterima, sehingga memunculkan kerentanan keamanan besar di luar kontrol langsung sistem keamanan lembaga perbankan (Damayanti & Priyono, 2022).

Dalam viktimologi, korban (victim) merupakan pihak yang mengalami kerugian baik secara langsung ataupun tidak langsung akibat tindak pidana. Nasabah korban phishing termasuk kategori korban pasif yang tidak mampu melindungi dirinya dari serangan digital karena tidak memiliki otoritas teknis terhadap sistem perbankan. Nasabah perbankan sering berada pada posisi secondary victim akibat kelalaian institusi keuangan dalam menjaga keamanan data. Analisis viktimologi menuntut agar orientasi perlindungan korban tidak hanya terfokus pada pemidanaan pelaku, tetapi juga pada pemulihan hak korban (Ardiansyah, 2023).

Perlindungan hukum bagi nasabah yang menjadi korban phishing harus memuat ruang preventif serta represif. Dimensi preventif berfokus pada kewajiban bank menjaga keamanan infrastruktur elektronik dan data nasabah, sedangkan dimensi represif diarahkan pada pertanggungjawaban hukum apabila timbul kerugian akibat kelemahan sistem keamanan maupun kelalaian pengawasan internal (Fadhilah & Taufiq Nugroho, 2025). Bank sebagai lembaga yang menghimpun serta menyalurkan dana masyarakat dalam operasionalnya, dengan nilai dana publik yang sangat besar, wajib berpegang pada prinsip kehati-hatian. Kesalahan kecil dalam pengelolaan dana publik berpotensi menimbulkan dampak fatal. Relasi bank bersama nasabah berada pada area hak dan kewajiban yang wajib dipatuhi dua belah pihak. Apabila satu pihak melakukan tindakan yang merugikan pihak lainnya melalui cara yang bertentangan dengan norma hukum perbankan, perbuatan tersebut termasuk tindak pidana perbankan atau tindak pidana dalam aktivitas perbankan (Zulfirman, 2025).

Persoalan inti dalam perkara phishing terletak pada bagaimana konstruksi perlindungan hukum terhadap korban phishing terkait data nasabah, khususnya keterkaitannya dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik atas kerugian finansial nasabah bank. Kondisi ini menciptakan kekhawatiran nasabah serta penurunan kepercayaan publik terhadap kemampuan bank dalam memberikan perlindungan hukum atas data nasabah sebagai penyedia layanan jasa perbankan, terlebih ketika terdapat kelalaian nasabah menjaga kerahasiaan data. Kompleksitas pembuktian digital semakin menambah urgensi untuk menelaah bentuk perlindungan hukum terhadap nasabah perbankan. Penelitian terkait perlindungan hukum korban phishing dalam sektor perbankan memiliki urgensi signifikan, tidak hanya untuk menguatkan sistem legislasi, tetapi juga untuk membangun kembali kepercayaan publik terhadap sistem keuangan nasional.

METODE PENELITIAN

Metode penelitian menggunakan desain penelitian kepustakaan, berupa pendekatan berbasis penelusuran literatur relevan guna membangun pemahaman mendalam mengenai perlindungan hukum terhadap nasabah bank di Indonesia pada kasus penipuan digital, pencurian data pribadi, serta phishing. Penulis menautkan sumber relevan terstruktur berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. Pendekatan statute fokus pada norma pada peraturan perundang-undangan terkait. Analisis dijalankan secara kualitatif melalui teknik interpretasi gramatikal, sistematis, serta teleologis dalam rangka membangun argumentasi hukum terkait perlindungan pelanggan dari phishing (Irwansyah, 2020). Data yang dipakai berupa data sekunder, mencakup materi hukum primer berupa KUHP, Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik, UU Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, serta aturan OJK dan sumber sekunder berupa buku serta jurnal relevan (Sampara & Husen, 2016).

HASIL DAN PEMBAHASAN

A. Perlindungan hukum terhadap Korban Phising

Pemikiran Satjipto Rahardjo menempatkan perlindungan hukum sebagai instrumen menjaga keseimbangan hak dan kewajiban sekaligus menghalangi tindakan yang berpotensi mengganggu keteraturan norma hukum positif. Perlindungan hukum tidak terbatas pada ranah fisik karena konsep tersebut turut menegaskan perlindungan atas kepentingan hukum subjek agar proses pemenuhan hak dapat berlangsung tanpa ancaman atau gangguan melawan hukum (Rahardjo, 2009).

Phishing yang diarahkan kepada nasabah bank di Indonesia bukan sekadar persoalan teknologi digital karena tindakan tersebut telah memenuhi unsur kejahatan siber dalam hukum nasional. Modus berupa penawaran palsu, informasi biaya transfer manipulatif, atau tautan penggantian kartu yang bersifat ilegal bertujuan memperoleh akses tanpa hak atau mengambil data rahasia nasabah. Tindakan tersebut melanggar Pasal 30 UU Nomor 11 Tahun 2008 mengenai akses ilegal sistem elektronik serta Pasal 28 Ayat (1) UU Nomor 1 Tahun 2024 terkait penyebaran informasi menyesatkan yang berdampak merugikan konsumen. Pemahaman phishing sebagai pelanggaran hukum merupakan pijakan penting untuk melihat posisi hubungan hukum antara bank, nasabah, serta ancaman digital eksternal (Erdiyanto, 2023).

Perkembangan digitalisasi memunculkan tantangan baru dalam sektor perbankan. Transformasi digital telah menjadi pemicu utama perubahan besar perbankan beberapa dekade terakhir. Teknologi informasi membuka peluang bank memperluas layanan, memberi kemudahan

kepada nasabah dalam melakukan transaksi finansial tanpa kehadiran fisik ke kantor cabang. Aktivitas transfer dana, pembayaran tagihan, hingga pengelolaan instrumen investasi dapat dijalankan melalui perangkat digital seperti smartphone atau komputer. Transformasi digital mendorong efisiensi, memudahkan proses transaksi, dan meningkatkan kualitas pengalaman pengguna secara komprehensif (Agusthin et al., 2024).

Bank digital menghadapi ancaman phishing melalui penerapan mitigasi terpadu berbasis keamanan informasi modern. Implementasi enkripsi data, autentikasi dua faktor, dan sistem pendeteksi aktivitas mencurigakan menjadi instrumen pertahanan yang menutup peluang penetrasi ke sistem perbankan digital. Edukasi nasabah memegang peran fundamental dalam meningkatkan kesadaran risiko agar mampu menghindari pesan atau tautan manipulatif yang berpotensi mengarah pada kompromi data kredensial. Audit keamanan berkala menjaga ketahanan sistem terhadap evolusi serangan digital lintas waktu. Kemitraan dengan regulator dan otoritas berfungsi membangun regulasi adaptif terhadap intensitas eskalasi kejahatan siber. Model mitigasi berlapis tersebut memperkuat kepercayaan publik serta menopang stabilitas intermediasi keuangan berbasis teknologi pada infrastruktur perbankan digital (Az-zahra & Labib, 2025).

POJK Nomor 3 Tahun 2023 mewajibkan bank digital mengintegrasikan program edukasi dalam perencanaan tahunan guna meningkatkan kapasitas literasi nasabah untuk memahami fungsi, prosedur, serta karakteristik layanan perbankan digital. Sosialisasi dilakukan melalui sinergi dengan institusi pemerintah, akademisi, dan pihak non pemerintah sebagai strategi distribusi pengetahuan kolektif mengenai keamanan digital. Bank digital mengimplementasikan pendekatan edukasi tersebut untuk memperkuat tata kelola keamanan teknologi keuangan serta meningkatkan pemahaman publik terhadap mekanisme mitigasi risiko pada layanan perbankan digital (Chairunnisa et al., 2024).

Pembuktian elemen kerugian dalam perkara phishing cenderung mudah karena tercermin melalui berkurangnya saldo dalam rekening nasabah. Perdebatan pembuktian kompleks biasanya terdapat pada hubungan kausal antara kelalaian bank dan kerugian finansial nasabah. Bank berpotensi berargumen bahwa sumber utama kerugian bersumber dari tindakan phisher atau kelemahan individu dalam memahami modus penipuan digital. Perspektif hukum tetap dapat menyusun hubungan kausal tersebut melalui penilaian terhadap kelemahan sistem keamanan bank atau rendahnya intensitas edukasi keamanan digital yang pada akhirnya berkontribusi signifikan dalam memfasilitasi serangan phishing. Pasal 58 Undang-Undang Nomor 27 Tahun 2022 memperkuat legal standing klaim pemulihan kerugian karena memberikan hak subjek data untuk memperoleh kompensasi atas pelanggaran perlindungan data pribadi (Shapiro, 2023).

Perlindungan terhadap korban phishing memegang peranan penting dalam menjaga legitimasi sistem perbankan digital. Pemikiran Satjipto Rahardjo menghadirkan pendekatan perlindungan kepada pihak yang rentan dalam relasi kuasa termasuk nasabah perbankan digital. Phishing dikonstruksikan sebagai cybercrime berdasarkan UU ITE dan UU PDP sehingga isu ini mencakup kewajiban pengendalian data oleh lembaga keuangan. Transformasi digital banking menghasilkan efisiensi transaksi sekaligus meningkatkan eskalasi ancaman manipulasi digital. Bank digital wajib menata standar kehati-hatian bukan hanya pada aspek teknis keamanan tetapi juga governance risiko, edukasi publik, audit keamanan, serta internal control berbasis pendekatan compliance berbasis risiko.

Regulasi OJK mempertegas kewajiban edukasi struktural dan sistematis sebagai instrumen perlindungan preventif. Kasus phishing memperlihatkan karakter pembuktian hukum yang kompleks, terutama dalam pembuktian hubungan kausalitas antara kelemahan bank dan kerugian finansial nasabah. Doktrin kausalitas dalam hukum perdata mengafirmasi bahwa kesempatan

terjadinya risiko yang timbul akibat kelalaian sistemik bank dapat menjadi dasar atribusi tanggung jawab hukum terhadap kerugian. Pasal 58 UU PDP menyediakan landasan gugatan keperdataan terhadap subjek pemroses data apabila terbukti kelalaian. Analisis kritis terhadap seluruh struktur tersebut menunjukkan perlindungan hukum bagi korban phishing membutuhkan pendekatan integral berbasis teori keadilan substantif, kejelasan norma, penegakan hukum non formalistik, serta de-dominasi kekuasaan lembaga finansial dalam relasi dengan konsumen.

B. Analisis Perlindungan Data Nasabah Bank korban cybercrime Phising

Perlindungan hukum atas data nasabah perbankan memiliki posisi sentral dalam konteks digitalisasi sektor keuangan modern. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana perubahan Undang-Undang Nomor 19 Tahun 2016 (UU ITE) menjadi landasan normatif utama bagi penegakan keamanan data elektronik termasuk data sektor perbankan. UU ITE berfungsi bukan sekadar memberi legitimasi penggunaan dokumen elektronik dalam praktik ekonomi, tetapi juga mengatur larangan serta sanksi terhadap setiap bentuk penyalahgunaan data pribadi nasabah perbankan.

Pasal 26 UU ITE menegaskan bahwa pemanfaatan data pribadi dalam sistem elektronik wajib bertumpu pada adanya persetujuan subjek data. Informasi berupa nomor rekening, identitas personal, password, serta one time password (OTP) termasuk kategori hak privasi nasabah yang berada dalam rezim perlindungan hukum positif. Dalam aktivitas digital banking, norma tersebut menjadi dasar kepatuhan lembaga perbankan untuk memastikan bahwa akses data pribadi nasabah berlangsung sesuai ketentuan sah sehingga meminimalkan risiko intrusi siber maupun pemrosesan ilegal atas data sensitif nasabah (Sari, 2020). Perlindungan terhadap nasabah korban kejahatan phishing pada praktik nasional masih mengalami defisit implementatif pada struktur hukum perbankan (Ekawati, 2018). Berbicara mengenai perlindungan terhadap nasabah bank, maka kita harus membedakan nasabah sebagai kreditur terhadap bank dan nasabah sebagai debitur terhadap bank yaitu :

1) Perlindungan secara implisit *(Implicit Deposit Protection)*
2) Perlindungan Secara Eksplisit *(Explicit Deposit Protection)*(Justin Thenata et al., 2025)

Perlindungan secara Implisit adalah perlindungan yang dihasilkan oleh pengawasan dan pembinaan bank yang efektif yang dapat menghindarkan terjadinya kebangkrutan bank yang diawasi (Schich, 2018). Perlindungan ini dapat diperoleh melalui:

1) Peraturan perundang-undangan di bidang Perbankan (Undang-undang Nomor 10 Tahun 1998).
2) Perlindungan yang dihasilkan oleh pengawasan dan pembinaan yang efektif yang dilakukan oleh Bank Indonesia
3) Upaya menjaga kelangsungan usaha bank sebagai suatu lembaga pada khususnya dan perlindungan terhadap sistem perbankan pada umumnya.
4) Memelihara tingkat kesehatan bank.
5) Melakukan usaha sesuai dengan prinsip kehati-hatian.
6) Cara pemberian kredit yang tidak merugikan bank dan kepentingan nasabah.
7) Menyediakan informasi resiko pada nasabah (Yustianti, 2017).

Perlindungan eksplisit berada pada ranah kebijakan kelembagaan yang menetapkan adanya badan penjamin simpanan masyarakat sehingga apabila terjadi kegagalan operasional bank, institusi tersebut berkewajiban memberikan penggantian atas dana pihak penyimpan (Suhardiono et al., 2025). Konsep perlindungan eksplisit dapat diimplementasikan melalui keberadaan Lembaga Penjamin Simpanan sebagaimana konstruksi teoretis dalam studi Diamond dan Dybvig (1983). Mekanisme Perlindungan Eksplisit yaitu :

1) Kerahasiaan Bank: bank dilarang membocorkan informasi nasabah tanpa izin. Jika terjadi akibat phishing, bank wajib bertanggung jawab atas keamanan sistem (Sjahdeini, 1999).
2) Sanksi Pidana Cybercrime: pelaku phishing dapat dijerat Pasal 30 & 32 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dengan ancaman pidana hingga 8 tahun.
3) Pengawasan OJK & BI: pengaturan keamanan siber masuk dalam regulasi POJK No. 38/POJK.03/2016 tentang Manajemen Risiko Teknologi Informasi dan SEOJK No. 29/SEOJK.03/2022 tentang Keamanan Siber Perbankan.
4) Perlindungan Konsumen: OJK melalui UU No. 21 Tahun 2011 memastikan perlindungan konsumen jasa keuangan, termasuk kasus phishing.

Pasal 30 Ayat 3 dan Pasal 46 mengenai sanksi yang lebih spesifik mengenai *Phising* Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik: "Setiap orang dengan sengaja dan tanpa hak mengakses komputer dan/atau sistem elektronik dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan."

Pasal 30 UU ITE menegaskan larangan akses sistem elektronik tanpa otorisasi pemilik sistem. Penegasan norma tersebut memiliki hubungan erat terhadap tindak phishing karena pelaku memperoleh akses ilegal ke akun perbankan digital melalui teknik pengelabuan korban. Norma ini berfungsi sebagai rintangan yuridis awal untuk menindak setiap upaya pembobolan sistem perbankan sebelum timbul kerugian finansial (Ninggeding et al., 2023). Sanksi Pasal 46 yang dimaksud adalah "Pelanggaran ayat (3) dipidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp 800 juta." Pasal 32 Ayat 1 menyebutkan mengenai Manipulasi atau Perusakan Data Elektronik: "Setiap orang dengan sengaja dan tanpa hak mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik."

Sanksi disebutkan Pasal 48 Ayat 1 yaitu "Pelanggaran ayat (1) dipidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp 2 miliar." Pasal 32 UU ITE memberikan proteksi lebih luas melalui pelarangan tindakan manipulasi, pemindahan, serta penyembunyian data elektronik. Kasus phishing dapat dikualifikasikan dalam norma tersebut karena pelaku memanfaatkan data curian untuk memindahkan saldo rekening atau menutupi jejak digital. Distribusi data hasil phishing ke jaringan kejahatan siber transnasional merupakan contoh nyata delik Pasal 32 ayat (2) sehingga keberadaan norma ini berperan strategis dalam menjaga integritas sistem perbankan digital (Amru et al., 2025). Pasal 32 Ayat (1) UU ITE memberikan dasar pemidanaan terhadap pelaku kejahatan siber karena perbuatan memindahkan atau mengubah data elektronik. Kejahatan phishing masuk dalam ruang lingkup tersebut karena pelaku tidak hanya mencuri data, tetapi sekaligus melakukan perubahan struktur data elektronik milik nasabah.

Perlindungan data nasabah bank korban phishing membutuhkan pendekatan korelatif antara norma perlindungan data, rejim perbankan, serta kerangka pidana siber yang telah berkembang dalam UU ITE. UU ITE menetapkan konstruksi legal privasi data berbasis consent sehingga basis akses informasional nasabah dalam transaksi digital perbankan berada pada zona hak eksklusif subjek data. Pembacaan terhadap norma ini menciptakan batas yuridis jelas bahwa data perbankan merupakan objek kepentingan hukum yang memiliki sifat strategis dalam transaksi finansial digital. Permasalahan terletak pada belum optimalnya penerjemahan norma perlindungan data dalam level operasional perbankan nasional terutama ketika nasabah menjadi korban phishing. Terdapat dualitas rezim perlindungan berupa perlindungan implisit melalui prudential banking regulation serta perlindungan eksplisit melalui skema penjaminan simpanan,

namun keduanya belum menyentuh secara presisi kerentanan korban phishing berbasis manipulasi sosial.

Bank cenderung memposisikan tanggung jawab pada kesalahan pelanggan padahal konstruksi risiko digital bersifat sistemik sehingga standar kehati-hatian perbankan wajib mencakup penguatan keamanan data melalui kebijakan TI berbasis risk management, kontrol akses berlapis, edukasi risiko, serta compliance teknis mengikuti POJK keamanan siber. Sanksi pidana dalam UU ITE terhadap akses ilegal dan manipulasi data elektronik telah menyediakan instrumen penjeraan, namun perlindungan substantif terhadap nasabah korban phishing masih membutuhkan penguatan enforcement dalam ranah perdata melalui mekanisme ganti rugi berbasis pelanggaran hak data pribadi. Analisis kritis menunjukkan perlindungan nasabah phishing akan efektif apabila dipahami sebagai isu data governance, bukan sekadar isu cybersecurity murni, sehingga perlu integrasi antara perlindungan konsumen, prudential regulation, dan penegakan hukum pidana berbasis perlindungan data.

C. Dimensi Perlindungan Untuk Nasabah Bank

Dimensi kewajiban bank semakin kuat pasca pengaturan perlindungan data pribadi dalam Undang-Undang Nomor 27 Tahun 2022. Posisi bank sebagai pengendali data menempatkan institusi keuangan pada tanggung jawab hukum penuh untuk memastikan seluruh proses pengelolaan data pribadi nasabah mencakup pengumpulan, penyimpanan, penggunaan, hingga pemusnahan dilakukan secara sah, adil, transparan, serta aman. Regulasi tersebut mewajibkan penerapan keamanan teknis dan organisasi sesuai tingkat risiko untuk mencegah akses ilegal, pengungkapan tidak sah, atau perubahan data pribadi termasuk kredensial perbankan yang menjadi sasaran utama phishing. Kewajiban menjaga kerahasiaan dan integritas data pribadi memiliki hubungan langsung dengan pencegahan phishing karena keberhasilan serangan bergantung pada akuisisi data sensitif pengguna layanan digital (Nur & Sukma, 2025). Ruang lingkup perlindungan hukum yang sangat luas terhadap intervensi tanpa otorisasi ke dalam sistem elektronik perbankan menempatkan manipulasi data digital melalui phishing sebagai bentuk pemenuhan unsur Pasal 32 terutama terkait pemindahan serta penyembunyian informasi elektronik (Az-zahra & Labib, 2025). Makna Hukum Pasal 32 Ayat (1) :

1) Penekanan dalam hal Objek perlindungan yang dimaksud adalah informasi elektronik dan/atau dokumen elektronik (data perbankan, identitas digital nasabah). bahwa data perbankan digital kini menjadi objek hukum yang dilindungi sama pentingnya dengan aset fisik.
2) Unsur perbuatan terlarang mencakup mengubah, menambah, mengurangi, menghilangkan, memindahkan, hingga menyembunyikan data elektronik.hal ini sangat relevan dengan praktik phishing di mana pelaku mencuri dan memindahkan data login nasabah untuk kepentingan keuangan illegal (Juita et al., 2023).

Dimensi perlindungan untuk nasabah bank dalam konteks kejahatan phishing berorientasi pada tanggung jawab hukum bank dalam mengelola seluruh siklus data pribadi sesuai UU 27 Tahun 2022. Peran bank tidak terbatas pada penyimpanan data, tetapi mencakup pengamanan, pengendalian akses, dan penerapan tata kelola data yang terukur berdasarkan level risiko. Kewajiban tersebut bertumpu pada prinsip lawful processing, akuntabilitas, serta keamanan data dengan desain preventif, karena serangan phishing memanfaatkan kelemahan pengelolaan data untuk memperoleh kredensial nasabah. Pasal 32 UU ITE memberikan sanksi terhadap manipulasi data elektronik dan memposisikan data elektronik setara dengan aset hukum material yang harus dilindungi secara ketat. Analisis ini menegaskan bahwa rezim perlindungan nasabah dalam banking digital tidak hanya mengandalkan pertanggungjawaban pidana terhadap pelaku phishing,

tetapi memperluas cakupan kewajiban kepada bank sebagai data controller untuk memastikan tidak tercipta celah risiko sistemik. Ketegasan pemaknaan Pasal 32 memperkuat legitimasi bahwa data perbankan merupakan objek hukum bernilai strategis yang wajib diproteksi dalam logika perlindungan risiko cyber modern berbasis keamanan, governance, dan kepastian hukum.

KESIMPULAN

Penelitian ini menghasilkan pemahaman hukum sistematis tentang kewajiban perbankan dalam menjaga integritas data nasabah pada konteks phishing dengan penekanan penegakan prinsip keamanan data sebagai bentuk perlindungan hukum. Argumen hukum mendefinisikan penguatan legal risk governance lembaga perbankan sebagai kontribusi substantif terhadap literatur hukum digital berbasis pendekatan konteks digitalisasi finansial modern. Implikasi penelitian memperluas horizon kajian hukum siber melalui penguatan konsep legal accountability perbankan berlandaskan perlindungan data pribadi dan prinsip risk based governance sektor keuangan. Kolaborasi lintas lembaga terkait diperlukan untuk membangun sistem perlindungan yang terkoordinasi dan responsif terhadap ancaman kejahatan siber seperti phishing dan kebocoran data pribadi. Perlunya peraturan teknis yang lebih operasional sebagai turunan dari UU PDP dan UU ITE yang mengatur mekanisme pelaporan insiden, standar keamanan siber, serta tanggung jawab hukum lembaga keuangan dalam menjaga kerahasiaan data nasabah. Selain itu, pembentukan pusat koordinasi perlindungan data nasabah di bawah pengawasan otoritas terkait dapat menjadi langkah strategis untuk mempercepat penanganan kasus dan meningkatkan efektivitas perlindungan hukum terhadap masyarakat. Arah penelitian lanjutan berorientasi pada pengembangan model evaluasi efektivitas enforcement UU PDP melalui pendekatan komparatif lintas yurisdiksi.

DAFTAR REFERENSI

Agusthin, I. D., Nada, D. C., & Putri, N. A. (2024). *Perlindungan Hukum Nasabah dari Kejahatan Phising dalam Layanan Perbankan Digital di Indonesia. Deposisi: Jurnal Publikasi Ilmu Hukum, 2 (4), 132–148*.

Amru, A., Adil, N., & Patilani, N. (2025). Perlindungan Hukum terhadap Penanggulangan Kejahatan Siber di Sektor Perbankan Digital Indonesia. *Journal of Scientech Research and Development*, *7*(1), 586–598.

Ardiansyah, R. (2023). Analisis Viktimologi terhadap Korban Cyber Crime Perbankan. *Jurnal Kriminologi Indonesia*, *19*(2), 77–92.

Az-zahra, I., & Labib, Z. M. (2025). Perlindungan Hukum bagi Nasabah dalam Kasus Phising dan Siber Perbankan di Indonesia. *Yurisprudentia: Jurnal Hukum Ekonomi*, *10*(2), 405–425.

Banjarnahor, A. C., & Priyana, P. (2022). Analisis Yuridis Cybercrime Terhadap Penanganan Kasus Phising Kredivo. *HERMENEUTIKA: Jurnal Ilmu Hukum*, *6*(1), 32–36.

Budhihartanti, C. (2020). Cyber Crime dalam Dunia Perbankan: Analisis Hukum dan Perlindungan Nasabah. *Jurnal Hukum & Pembangunan*, *50*(3), 455–473.

Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024). Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phising dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *2*(1), 1–16.

Damayanti, M., & Priyono, E. A. (2022). Legal Consequences for LDMO Disclosing Personal Data of Transacting Parties: A Study of Legal Protection. *SIGn Jurnal Hukum*, *4*(2), 221–232.

Diamond, D. W., & Dybvig, P. H. (1983). Bank runs, deposit insurance, and liquidity. *Journal of Political Economy*, *91*(3), 401–419.

Ekawati, D. (2018). Perlindungan hukum terhadap nasabah bank yang dirugikan akibat kejahatan skimming ditinjau dari perspektif teknologi informasi dan perbankan. *UNES Law Review*, *1*(2), 157–171.

Erdiyanto, R. P. (2023). Penipuan Mengatasnamakan Bank Berbentuk Phising. *Jurnal Inovasi Global*, *1*(2), 71–79.

Fadhilah, C. N., & Taufiq Nugroho, S. H. (2025). *Pertanggungjawaban Bank Atas Hilangnya Dana Nasabah Akibat Phising Berdasarkan Peraturan OJK Nomor 1/POJK. 07/2013*. Universitas Muhammadiyah Surakarta.

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

Juita, S. R., Astanti, D. I., & Septiandani, D. (2023). Perlindungan Hukum Terhadap Nasabah Bank Korban Kejahatan Skimming. *Jurnal USM Law Review*, *6*(1), 407–419.

Justin Thenata, P. D., Susanto, R. J., Kurniawati, J. O., & Lee, J. C. (2025). Analisis Tanggung Jawab Hukum Terhadap Keamanan Perbankan Dan Nasabah Dalam Kasus Phishing. *Cerdika: Jurnal Ilmiah Indonesia*, *5*(4).

Lendo, Y. T. (2025). Kajian Yuridis terhadap Kejahatan Pembobolan Rekening dalam Kasus Phishing di Sektor Perbankan. *LEX PRIVATUM*, *15*(5).

Ninggeding, N. Y., Bayuaji, R., & Indriastuty, D. E. (2023). Penegakan Hukum Terhadap Cyber Crime Di Bidang Perbankan Di Indonesia. *Jurnal Ilmu Hukum Wijaya Putra*, *1*(2), 215–224. https://doi.org/10.38156/jihwp.v1i2.107

Nur, M. S. M., & Sukma, D. P. (2025). Analisis Perlindungan Hukum Dan Tanggung Jawab Perdata Bank Terhadap Nasabah Korban Phishing Berdasarkan Undang-Undang No. 8 Tahun 1999. *Verstek*, *13*(3), 501–516.

Rahardjo, S. (2009). *Hukum Dalam Jagat Ketertiban*. Huma.

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

Sari, D. (2020). Perlindungan data pribadi dalam perspektif UU ITE. *Jurnal Legislasi Indonesia*, *17*(3), 345–360.

Schich, S. (2018). Implicit bank debt guarantees: costs, benefits and risks: implicit bank debt guarantees. *Journal of Economic Surveys*, *32*(5), 1257–1291. https://doi.org/10.1111/joes.12287

Shapiro, S. (2023). *Fancy bear goes phishing: The dark history of the information age, in five extraordinary hacks*. Random House.

Sjahdeini, S. R. (1999). *Perlindungan Nasabah dan Kerahasiaan Bank*. UI Press.

Suhardiono, S., Sembel, R., & Suwandi, S. (2025). Peran Lembaga Penjamin Simpanan dalam Menjaga Stabilitas Sektor Perbankan di Indonesia: Systematic Literature Review. *Ekonomis: Journal of Economics and Business*, *9*(1), 146–155.

Yustianti, S. (2017). Kewenangan pengaturan dan pengawasan perbankan oleh Bank Indonesia dan Otoritas Jasa Keuangan (OJK). *ACTA DIURNAL Jurnal Ilmu Hukum Kenotariatan*, *1*(1), 60–72.

Zulfirman, Z. (2025). Evaluasi Penerapan Undang-Undang Perbankan Terhadap Tindak Pidana Kredit Macet di PT Bank Rakyat Indonesia KCP Lubuk Basung. *Sumbang12 Law Journal*, *3*(2), 140–151.