Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 2, 2026
DOI: https://doi.org/10.61104/alz.v4i2.5073

Perlindungan Hukum Bagi Pengguna M-Banking Terhadap Pembobolan Dana Nasabah Ditinjau Dari UU No.1 Tahun 2024 Dan KUHP

Citra Ayu Nirmala[1], Dwikari Nuristiningsih[2], Marlinah[3]
Universitas Prof. Dr. Hazairin SH, Indonesia[1-3]
Email Korespondensi: citraayunirmala10@gmail.com

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Februari 2026, Article published: 28 Maret 2026

ABSTRACT
The advancement of digital technology has played a major role in the massive transformation in the banking world. Mobile banking has emerged and changed the way customers interact with financial services. Behind the convenience and speed offered by mobile banking, there is a big challenge that continues to haunt the digital banking world in the form of cybercrime. This study uses a normative research method or doctrinal legal research which aims to analyze the legal norms contained in laws and regulations, legal theories, and legal doctrines relevant to the problem being studied. Legal protection for mobile banking users is regulated in Law No. 1 of 2024 concerning Information and Electronic Transactions and Article 362 of the Criminal Code. Although regulations are available, their implementation faces obstacles in the form of limited user understanding, the capacity of law enforcement officers, and the complexity of evidence due to the digital nature of stolen objects. Legal protection for mobile banking users according to Law No. 1 of 2024 concerning Information and Electronic Transactions and the Criminal Code requires strategic steps, such as the development of multidisciplinary studies of law and technology, updating the legal curriculum, and increasing digital literacy. Strengthening the capacity of officers, collaboration between institutions, and harmonization of regulations are also important. Affirmation of the responsibility of electronic system organizers and restitution mechanisms is the key to realizing fair, effective and adaptive legal protection in the digital era.
Keywords: *Legal protection, cybercrime, customer fund theft*

ABSTRAK
Kemajuan teknologi digital mempunyai peranan besar terhadap transformasi besar besaran dalam dunia perbankan. Mobile banking muncul dan mengubah cara nasabah berinteraksi dengan layanan keuangan. Di balik kemudahan dan kecepatan yang ditawarkan mobile banking, tersembunyi satu tantangan besar yang terus menghantui dunia perbankan digital berupa cybercrime, atau kejahatan siber. Penelitian ini menggunakan metode penelitian normatif atau penelitian hukum doktrinal yang bertujuan untuk menganalisis norma-norma hukum yang terkandung dalam peraturan perundang-undangan, teori-teori hukum, serta doktrin hukum yang relevan dengan masalah yang diteliti. Perlindungan hukum terhadap pengguna mobile banking diatur dalam UU No. 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik dan Pasal 362 KUHP. Meskipun regulasi telah tersedia, implementasinya menghadapi kendala berupa keterbatasan pemahaman pengguna, kapasitas aparat penegak hukum, serta kompleksitas pembuktian akibat sifat digital objek yang dicuri. Perlindungan hukum terhadap pengguna mobile banking menurut UU No. 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik dan KUHP memerlukan langkah strategis,

seperti pengembangan kajian multidisipliner hukum dan teknologi, pembaruan kurikulum hukum, serta peningkatan literasi digital. Penguatan kapasitas aparat, kolaborasi antarlembaga, dan harmonisasi regulasi juga penting. Penegasan tanggung jawab penyelenggara sistem elektronik serta mekanisme restitusi menjadi kunci mewujudkan perlindungan hukum yang adil, efektif, dan adaptif di era digital.
Kata Kunci: *Perlindungan hukum, kejahatan siber, pembobolan dana nasabah*

PENDAHULUAN

Perkembangan teknologi telah menjadi salah satu faktor dominan yang membentuk arah dan wajah peradaban manusia modern. Digitalisasi, yang merupakan ciri utama perkembangan teknologi saat ini, telah membawa perubahan besar dalam berbagai bidang seperti pendidikan, ekonomi, pemerintahan, kesehatan, hingga gaya hidup masyarakat. Teknologi telah membentuk suatu ekosistem sosial yang baru, di mana individu dan kelompok masyarakat menjalani kehidupan sehari-hari dalam interaksi yang terus-menerus dengan sistem digital. Teknologi telah membentuk suatu ekosistem sosial yang baru, di mana individu dan kelompok terus-menerus dengan sistem digital. Transformasi ini menunjukkan bahwa teknologi bukan hanya hasil dari perkembangan ilmu pengetahuan, tetapi juga menjadi agen perubahan sosial yang mendalam. Dalam konteks tersebut, memahami perkembangan teknologi bukan sekadar menyoroti aspek teknis atau inovatifnya, melainkan juga melihatnya sebagai proses integral dalam evolusi masyarakat menuju tatanan yang lebih adaptif, efisien, dan terhubung.

Kemajuan teknologi digital juga mempunyai peranan besar terhadap transformasi besar besaran dalam dunia perbankan. Perubahan gaya hidup masyarakat yang semakin bergantung pada perangkat mobile memicu bank-bank di seluruh dunia untuk beradaptasi dan menghadirkan layanan yang lebih praktis, cepat, dan aman.

Di tengah tuntutan efisiensi dan kenyamanan, *mobile banking* muncul sebagai solusi revolusioner yang mengubah cara nasabah berinteraksi dengan layanan keuangan. *Mobile banking* adalah layanan yang memungkinkan nasabah untuk melakukan berbagai transaksi perbankan melalui perangkat mobile seperti ponsel pintar atau tablet. Dengan menggunakan aplikasi *mobile banking* yang disediakan oleh bank, nasabah dapat mengakses akun mereka untuk melakukan berbagai aktivitas, seperti pengecekan saldo, transfer antar rekening, pembayaran tagihan, pembelian pulsa, pembelian tiket, serta investasi dan pembelian produk keuangan lainnya. Layanan ini dirancang untuk memudahkan nasabah dalam mengelola keuangan secara praktis dan efisien tanpa harus mengunjungi cabang bank secara fisik.

Mobile banking dalam system perbankan saat ini juga telah dilengkapi dengan berbagai lapisan keamanan informasi yang dirancang untuk melindungi aplikasi perbankan dan data pelanggan. Model keamanan ini terdiri dari berbagai solusi dan mekanisme yang berfungsi untuk memastikan identifikasi, otentikasi, dan otorisasi yang aman bagi pengguna. Beberapa komponen penting dalam sistem keamanan perbankan online meliputi penggunaan sertifikat digital untuk memvalidasi keabsahan antara pengguna dan sistem perbankan, yang bergantung pada *Public Key*

Infrastructure (PKI) dan *Certificate Authority* (CA) yang terpercaya. Selain itu, penggunaan kartu kata sandi satu kali (OTP) menawarkan kata sandi dinamis dan verifikasi kedua yang meningkatkan keamanan transaksi. Perlindungan browser memonitor ruang memori untuk mencegah malware yang dapat mencuri informasi sensitif, sementara keyboard virtual dirancang untuk mencegah pencatatan data yang dimasukkan melalui perangkat keras. Metode lain seperti pendaftaran perangkat dan identifikasi perangkat membatasi akses hanya kepada perangkat yang telah terdaftar, sementara *CAPTCHA* memastikan bahwa pengguna yang mengakses sistem adalah manusia dan bukan program komputer otomatis. Layanan pesan singkat (SMS) juga digunakan untuk memberikan verifikasi tambahan melalui pesan teks yang dikirimkan kepada nasabah sebagai langkah keamanan. Dengan menggabungkan berbagai mekanisme ini, sistem perbankan online dapat memberikan perlindungan yang lebih kuat terhadap serangan dan ancaman dunia maya, serta meningkatkan keamanan data pelanggan secara keseluruhan.

Di balik kemudahan dan kecepatan yang ditawarkan *mobile banking*, tersembunyi satu tantangan besar yang terus menghantui dunia perbankan digital berupa *cybercrime*, atau kejahatan siber. *Cybercrime* atau kejahatan siber merupakan istilah yang merujuk pada berbagai tindakan kriminal yang melibatkan penggunaan komputer, jaringan, atau internet sebagai alat utama dalam menjalankan aksinya. Aktivitas ini mencakup tindakan ilegal seperti peretasan, pencurian identitas, phishing, hingga serangan *ransomware*, yang bertujuan untuk mencuri data, uang, atau aset digital lainnya. Salah satu bentuk kejahatan siber yang paling merugikan adalah pembobolan dana nasabah, di mana pelaku memanfaatkan celah keamanan atau kelengahan pengguna untuk mengakses rekening dan mencuri uang secara ilegal. Pembobolan merujuk pada suatu tindakan atau proses yang dilakukan untuk merusak atau menerobos suatu sistem secara paksa.

Meskipun sistem perbankan modern memiliki keamanan canggih, risiko pembobolan dan serangan siber tetap ada. Pembobolan termasuk tindak pidana pencurian karena melibatkan pengambilan barang milik orang lain secara sengaja dan melawan hukum dengan niat menguasai tanpa izin. Tindakan ini menyebabkan peralihan kepemilikan secara tidak sah dan merugikan korban secara materiil maupun psikologis. Pencurian diatur dalam Pasal 362 KUHP dengan ancaman pidana penjara maksimal lima tahun atau denda maksimal sembilan ratus ribu rupiah. Dalam hal pembobolan dana dilakukan pada *mobile banking*, maka tindak pidana ini juga termasuk kedalam *cybercrime* yang diatur dalam UU No. 1 Tahun 2024 pasal 30 tentang Perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mengatur tentang larangan mengakses komputer dan/atau sistem elektronik milik orang lain tanpa izin atau secara melawan hukum.

Salah satu kasus pembobolan dana nasabah yang pernah terjadi adalah kasus yang dilakukan oleh mantan karyawan bank itu sendiri. Polda Metro Jaya telah menangkap seorang mantan pegawai bank digital berinisial IA (33) yang diketahui melakukan pembobolan terhadap 112 rekening nasabah yang sebelumnya dibekukan karena diduga menerima dana hasil tindak pidana. Pelaku berhasil mengakses dan menguras dana hingga mencapai total Rp1,3 miliar dengan

memanfaatkan jabatannya sebagai contact center specialist. Dalam praktiknya, IA memerintahkan agen command center untuk mengajukan permintaan pembukaan blokir, lalu menyetujui permintaan tersebut secara sepihak—sebuah tindakan yang termasuk dalam kewenangannya di bank tersebut. Aksi ilegal ini dilakukan selama periode 18 Maret hingga 31 Oktober 2023, dan menyebabkan kerugian pada pihak bank sebesar kurang lebih Rp1.397.280.711. Atas perbuatannya, IA dijerat dengan Pasal 30 ayat (1) jo. Pasal 46 ayat (1) dan/atau Pasal 32 ayat (1) jo. Pasal 48 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), serta/atau Pasal 81 Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana, dan/atau Pasal 3, Pasal 4, serta Pasal 5 Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (TPPU).

Berdasarkan uraian diatas, artikel ini akan mengkaji tentang bagaimana perlindungan hukum bagi pengguna *mobile banking* terhadap pembobolan dana nasabah ditinjau dari UU No. 1 Tahun 2024 tentang informasi dan transaksi elektronik dan bagaimana perlindungan hukum bagi pengguna *mobile banking* terhadap pembobolan dana nasabah ditinjau dari Kitab Undang-Undang Hukum Pidana.

METODE

Metode Penelitian adalah cara ilmiah yang digunakan untuk memperoleh data dengan tujuan dan kegunaan tertentu. Metode penelitian harus memenuhi tiga unsur utama yaitu cara ilmiah, data empiris yang objektif, dan tujuan tertentu, seperti untuk memahami, menjelaskan, atau memecahkan suatu permasalahan. Penelitian ini menggunakan metode penelitian normatif atau penelitian hukum doktrinal yang bertujuan untuk menganalisis norma-norma hukum yang terkandung dalam peraturan perundang-undangan, teori-teori hukum, serta doktrin hukum yang relevan dengan masalah yang diteliti. Penelitian ini tidak melibatkan pengumpulan data empiris, tetapi lebih kepada pengkajian atas peraturan yang berlaku dan analisis terhadap perlindungan hukum bagi korban kejahatan siber, khususnya pembobolan mobile banking, baik berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP) maupun UU No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE). Dalam penelitian ini, penulis menggunakan pendekatan hukum normatif *(normative approach*) yang berupa Pendekatan Perundang-Undangan (*Statute Approach*) dan Pendekatan Komparatif (*Comparative Approach)*. Pendekatan ini digunakan untuk menelaah peraturan perundang-undangan yang relevan dalam konteks hukum positif yang berlaku di Indonesia, yaitu UU No. 1 Tahun 2024 dan KUHP, khususnya pasal 362. Dalam pendekatan ini, penelitian juga berfokus pada analisis perbandingan kedua Undang-Undang tersebut dalam memberikan perlindungan kepada pengguna mobile banking terhadap pembobolan dana nasabah. Penelitian ini menggunakan tiga sumber data, yaitu sumber data primer berupa Kitab Undang-Undang Hukum Pidana (KUHP) yang merupakan peraturan perundang-undangan utama yang mengatur tindak pidana pencurian, yang dijadikan acuan untuk melihat relevansi dalam menangani kasus pembobolan *mobile banking*. Undang-Undang No. 1 Tahun 2024 tentang

Informasi dan Transaksi Elektronik (UU ITE) yang mengatur kejahatan siber, termasuk akses ilegal, pencurian data, dan manipulasi sistem elektronik, yang sangat relevan dalam konteks pembobolan *mobile banking*. Bahan hukum sekunder yang berupa nuku-buku hukum membahas tentang teori hukum, hukum pidana, dan cybercrime. Jurnal dan artikel ilmiah yang membahas penerapan hukum di bidang teknologi informasi dan *cybercrime,* serta perlindungan hukum bagi korban kejahatan siber. Dokumen terkait seperti literatur akademik, hasil penelitian sebelumnya, serta artikel yang relevan dengan tema penelitian ini. Dan bahan hukum tersier berupa kamus, Kamus Bahasa Indonesia, Kamus Hukum, dan Ensiklopedi.

Dalam penelitian ini, teknik pengumpulan data yang digunakan adalah studi pustaka dengan mengumpulkan berbagai literatur, baik itu peraturan perundang-undangan, putusan pengadilan, maupun referensi akademik yang relevan dengan topik penelitian. Menelaah buku, artikel, dan jurnal yang membahas mengenai perlindungan hukum terhadap korban kejahatan siber, pencurian, serta penerapan KUHP dan UU ITE dalam praktik hukum di Indonesia dan studi dokumen dengan mengumpulkan dan menganalisis dokumen hukum yang berkaitan dengan cybercrime, seperti peraturan perundang-undangan, peraturan pemerintah, dan keputusan pengadilan terkait. Menganalisis data hukum yang tersedia untuk mengidentifikasi celah-celah hukum yang perlu diperbaiki, serta mengevaluasi sejauh mana peraturan perundang-undangan tersebut memberikan perlindungan yang memadai bagi korban kejahatan siber. Pengolahan bahan hukum adalah langkah-langkah yang dilakukan untuk mengorganisasikan dan menganalisis bahan-bahan hukum yang telah terkumpul, agar dapat memberikan hasil yang jelas dan relevan dalam menjawab rumusan masalah penelitian. Dalam penelitian normatif, bahan-bahan hukum yang digunakan adalah peraturan perundang-undangan dan doktrin hukum yang kemudian diolah agar dapat dipahami dan diinterpretasikan sesuai dengan tujuan penelitian. Data yang diperoleh dari penelitian ini akan dianalisis dengan menggunakan teknik analisis kualitatif, yang berfokus pada penafsiran dan analisis terhadap peraturan perundang-undangan dan teori-teori hukum yang ada. Langkah-langkah analisis data yang dilakukan adalah dengan menganalisis isi dari Pasal 362 KUHP dan UU ITE, serta mengidentifikasi relevansi dan kelemahan-kelemahan yang ada dalam kedua undang-undang tersebut terkait perlindungan korban kejahatan siber.

HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa pembobolan dana yang dilakukan melalui *mobile banking* termasuk kedalam *cybercrime* yang diatur dalam UU No. 1 Tahun 2024 pasal 30 tentang Perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mengatur tentang larangan mengakses komputer dan/atau sistem elektronik milik orang lain tanpa izin atau secara melawan hukum. Beberapa ayat pada pasal ini menjelaskan lebih lanjut mengenai Tindakan yang termasuk kedalamnya, antara lain:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.
(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Sanksi pidananya diatur dalam pasal 40 yang berbunyi:
(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Dalam pasal 52 ayat (3) juga disebutkan ketentuan tambahan yakni Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap komputer dan/atau sistem elektronik serta Informasi elektronik dan/atau dokumen elektronik milik pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.

Secara normatif, undang-undang ini memberikan jaminan perlindungan hukum bagi pengguna layanan digital, termasuk nasabah mobile banking. Ketentuan dalam UU ITE mengatur prinsip-prinsip dasar transaksi elektronik yang mencakup keabsahan dokumen digital, pengakuan atas tanda tangan elektronik, serta perlindungan atas data pribadi yang diproses oleh penyelenggara sistem elektronik (PSE), dalam hal ini termasuk lembaga perbankan digital. UU No. 1 Tahun 2024 menempatkan tanggung jawab hukum pada pihak penyelenggara sistem elektronik untuk menjamin keandalan sistem, menjaga integritas serta kerahasiaan data, dan mencegah segala bentuk akses ilegal terhadap sistem informasi. Tindak pidana seperti akses tanpa hak terhadap sistem elektronik, intersepsi ilegal, dan manipulasi data diatur secara tegas dan disertai ancaman pidana serta denda. Dengan demikian, Undang – Undang ini telah menyediakan perangkat hukum yang memadai untuk memberikan perlindungan terhadap konsumen jasa keuangan digital.

Namun pada tataran implementasi, berbagai kendala struktural dan kultural menghambat efektivitas perlindungan hukum tersebut. Salah satu tantangan utama terletak pada rendahnya tingkat literasi digital masyarakat. Sebagian besar pengguna mobile banking belum memiliki kesadaran dan pengetahuan yang cukup terkait keamanan siber dan protokol perlindungan data pribadi. Kondisi ini diperburuk oleh praktik perbankan yang belum sepenuhnya transparan dalam

memberikan edukasi kepada nasabah tentang potensi risiko digital dan mekanisme pengaduan apabila terjadi insiden keamanan. Di sisi lain, penegakan hukum terhadap kejahatan siber sering kali menghadapi keterbatasan teknis dan yurisdiksional. Aparat penegak hukum, termasuk kepolisian dan kejaksaan, masih menghadapi tantangan dalam aspek teknis forensik digital, pelacakan transaksi, dan pembuktian elektronik yang kompleks. Lebih jauh, karena sebagian besar kejahatan digital melibatkan pelaku lintas negara, dibutuhkan kerangka kerja sama internasional yang kuat, baik secara bilateral maupun multilateral, yang saat ini masih belum berjalan optimal.

Dinamika perkembangan teknologi digital yang begitu cepat juga menyebabkan regulasi kerap kali tertinggal dalam merespons munculnya modus-modus baru dalam kejahatan digital. Inkonsistensi antara regulasi nasional dan kebijakan internal lembaga keuangan juga menambah kerumitan. Misalnya, tidak semua bank memiliki kebijakan kompensasi yang jelas bagi nasabah yang menjadi korban kejahatan digital, sehingga menimbulkan ketidakpastian hukum dan rasa ketidakadilan bagi korban.

Dari sudut pandang hukum perlindungan konsumen, ini menunjukkan adanya ketimpangan posisi antara lembaga perbankan sebagai penyelenggara sistem dan nasabah sebagai pengguna layanan. Meskipun secara yuridis formal perlindungan telah diberikan, secara sosiologis dan praktis masih terdapat kesenjangan dalam pelaksanaannya. Oleh karena itu, diperlukan pendekatan holistik yang mencakup reformasi regulasi, peningkatan kapasitas lembaga penegak hukum, penguatan pengawasan terhadap industri perbankan digital, serta kampanye literasi digital yang masif untuk meningkatkan kesadaran masyarakat sebagai subjek hukum dalam ruang digital.

Dengan demikian, perlindungan hukum terhadap pengguna mobile banking di bawah UU ITE tidak dapat dilihat hanya sebagai norma yang tertulis, tetapi harus dipahami sebagai suatu ekosistem perlindungan yang melibatkan interaksi antara norma hukum, kebijakan teknis, kelembagaan, dan budaya digital masyarakat. Tanpa penguatan pada aspek implementasi, perlindungan hukum akan tetap bersifat deklaratif dan belum mampu memenuhi prinsip keadilan substantif bagi seluruh pengguna layanan keuangan digital di Indonesia.

Selain itu, Pembobolan dana nasabah dalam konteks perbankan dapat dikategorikan sebagai tindak pidana pencurian karena memenuhi unsur-unsur yang terdapat dalam pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP), yaitu perbuatan mengambil barang milik orang lain tanpa hak dan melawan hukum. Dalam hal ini, barang yang dimaksud adalah dana atau informasi milik nasabah, yang diambil secara sengaja dengan niat untuk menguasai tanpa izin dari pemilik yang sah. Dalam banyak kasus, pelaku menggunakan teknik tertentu, seperti *hacking*, *skimming*, atau *phishing*, untuk mendapatkan akses ilegal ke informasi nasabah. Kejahatan ini seringkali dilakukan dengan upaya untuk menghindari deteksi atau penangkapan, serta tanpa sepengetahuan atau izin dari pemilik dana tersebut.

Akibat dari perbuatan ini adalah peralihan kepemilikan yang tidak sah, yang merugikan korban, baik secara materiil maupun psikologis. Korban tidak hanya

mengalami kerugian finansial, tetapi juga dapat merasakan dampak psikologis akibat hilangnya kepercayaan terhadap sistem perbankan. Dalam konteks hukum, tindak pidana ini diatur dalam pasal 362 KUHP yang menyatakan bahwa "Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak sembilan ratus rupiah." Hal ini menunjukkan bahwa tindak pencurian dalam ranah perbankan harus dipandang serius dan ditindaklanjuti sesuai dengan peraturan yang berlaku.

Secara normatif, rumusan pasal ini menetapkan sejumlah unsur yang harus dipenuhi, yaitu: (1) adanya perbuatan mengambil, (2) objek yang diambil adalah barang milik orang lain, (3) dilakukan dengan maksud untuk memiliki secara melawan hukum.

Dalam kasus pembobolan rekening melalui mobile banking, unsur-unsur ini secara substansial dapat ditemukan. Tindakan pelaku yang mengakses sistem perbankan secara ilegal, lalu memindahkan sejumlah dana dari rekening korban ke rekening pelaku atau pihak lain, pada hakikatnya merupakan bentuk pengambilan harta milik orang lain dengan niat melawan hukum. Oleh karena itu, tindakan tersebut dapat dikualifikasikan sebagai pencurian sebagaimana dimaksud dalam Pasal 362 KUHP.

Namun demikian, permasalahan muncul ketika tindakan tersebut dihadapkan pada sifat *nonfisik* dari objek yang dicuri, yakni dana elektronik. Uang dalam bentuk digital bukanlah "barang" dalam pengertian konvensional sebagaimana dimaksud dalam hukum pidana klasik. Ini menimbulkan problematika interpretatif, karena unsur "barang" dalam Pasal 362 secara historis merujuk pada objek yang bersifat tangible (berwujud). Akibatnya, timbul perdebatan apakah dana elektronik atau saldo rekening digital dapat dikategorikan sebagai objek pencurian dalam konstruksi hukum pidana yang bersifat klasik.

Kompleksitas ini bertambah dengan tantangan dalam proses pembuktian. Kejahatan berbasis transaksi digital sering kali melibatkan jaringan teknologi yang canggih, termasuk penggunaan rekayasa sosial, pemalsuan data digital, dan perangkat lunak peretas (malware). Pembuktian atas unsur "pengambilan" dalam sistem digital tidak dapat dilakukan dengan cara yang sama seperti pencurian fisik. Dibutuhkan pendekatan pembuktian berbasis forensik digital dan kemampuan aparat penegak hukum dalam menganalisis log sistem serta jejak transaksi elektronik.

Meskipun demikian, dalam praktik yurisprudensi dan penegakan hukum, Pasal 362 tetap dapat digunakan sebagai dasar pemidanaan terhadap pelaku pembobolan rekening, dengan pendekatan interpretatif yang lebih progresif. Beberapa pengadilan telah memperluas makna "barang" untuk mencakup aset digital, dengan merujuk pada nilai ekonomis dan kepemilikan sah atas dana elektronik tersebut. Pendekatan ini sejalan dengan perkembangan hukum pidana modern yang mulai mengakomodasi realitas baru dalam dunia digital.

Oleh karena itu, meskipun secara normatif Pasal 362 KUHP bukanlah peraturan yang secara khusus dirancang untuk menghadapi kejahatan siber, pasal

ini tetap dapat dijadikan sebagai landasan hukum yang relevan dalam menjerat pelaku pembobolan mobile banking. Namun, efektivitasnya sangat bergantung pada keberanian interpretatif aparat penegak hukum serta ketersediaan alat bantu teknologi untuk pembuktian digital. Di sisi lain, hal ini juga menegaskan pentingnya pembaruan hukum pidana nasional agar lebih adaptif terhadap perkembangan teknologi informasi dan perubahan bentuk-bentuk kejahatan modern.

SIMPULAN

Kesimpulan yang didapat adalah Perlindungan hukum bagi pengguna *mobile banking* ditinjau dari Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) telah diberikan melalui regulasi yang yang komprehensif terkait transaksi elektronik dan kejahatan siber, termasuk pembobolan dana melalui *mobile banking*, tetapi faktor-faktor seperti kurangnya pemahaman pengguna, keterbatasan aparat penegak hukum, dan perkembangan teknologi yang cepat bisa menjadi penghambat pelaksanaan perlindungan hukum secara optimal. Selanjutnya, perlindungan hukum bagi pengguna *mobile banking* ditinjau dari Kitab Undang-Undang Hukum pidana khususnya pada Pasal 362 yang mengatur tentang tindak pidana pencurian telah diberikan melaui regulasi yang ada. Adapun hal ini didukung karena faktor-faktor yang ada dalam pasal ini telah terpenuhi dalam kasus pembobolan dana nasabah. Namun dalam konteks pembobolan *mobile banking* yang berbasis transaksi digital, penerapan pasal ini menjadi kompleks karena objek yang dicuri adalah dana elektronik, sehingga menimbulkan tantangan dalam interpretasi hukum dan pembuktian unsur-unsurnya. Meski demikian, pasal ini dapat menjadi landasan yang baik dalamr menegakkan perlindungan hukum bagi pengguna *mobile banking* terhadap pembobolan dana nasabah.

DAFTAR RUJUKAN

Akbar, R., & Nasution, M. I. P. (2024). Analisis Keamanan Data Pada Aplikasi Mobile Banking. *Journal of Sharia Economics Scholar (JoSES)*, *2*(2).

Arifah, Dista Amalia. "Kasus cybercrime di indonesia." *jurnal Bisnis dan Ekonomi* 18.2 (2011).

Kusumawati, D. E., & Wijaya, S. (2018). Pengaruh mobile banking terhadap kepuasan nasabah. *Jurnal Akuntansi & Bisnis, 19*(2), 112-121.

Ningrum, Delvyan Putri Surya, and Jamiatur Robekha. "Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking di Indonesia." *Journal Evidence Of Law* 1.1 (2022): 112-128

Nugroho, A. (2013). *Analisis dan Pencegahan Malware dalam Jaringan Komputer*. Jurnal Informatika dan Komputer, 15(2), 45–53.

Prasetya, T. & Rakhman, H. (2017). Keamanan Sistem Mobile Banking: Tantangan dan Solusi di Indonesia. *Jurnal Teknologi dan Sistem Keamanan, 12*(4), 99-108.

Ratulangi, C. H. (2021). Tindak pidana cyber crime dalam kegiatan perbankan. *Lex Privatum*, *9*(5).

Suwiknyo, F. B. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. *Lex Privatum*, *9*(4).

Tampubolon, W. S. (2016). Upaya Perlindungan Hukum Bagi Konsumen Ditinjau Dari Undang Undang Perlindungan Konsumen. *Jurnal Ilmiah Advokasi*, *4*(1), 53-61.

Akbar, R., & Nasution, M. I. P. (2024). Analisis Keamanan Data Pada Aplikasi Mobile Banking. *Journal of Sharia Economics Scholar (JoSES)*, *2*(2).

Arifah, Dista Amalia. "Kasus cybercrime di indonesia." *jurnal Bisnis dan Ekonomi* 18.2 (2011).

Kusumawati, D. E., & Wijaya, S. (2018). Pengaruh mobile banking terhadap kepuasan nasabah. *Jurnal Akuntansi & Bisnis, 19*(2), 112-121.

Ningrum, Delvyan Putri Surya, and Jamiatur Robekha. "Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking di Indonesia." *Journal Evidence Of Law* 1.1 (2022): 112-128

Nugroho, A. (2013). *Analisis dan Pencegahan Malware dalam Jaringan Komputer*. Jurnal Informatika dan Komputer, 15(2), 45–53.

Prasetya, T. & Rakhman, H. (2017). Keamanan Sistem Mobile Banking: Tantangan dan Solusi di Indonesia. *Jurnal Teknologi dan Sistem Keamanan, 12*(4), 99-108.

Ratulangi, C. H. (2021). Tindak pidana cyber crime dalam kegiatan perbankan. *Lex Privatum*, *9*(5).

Suwiknyo, F. B. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. *Lex Privatum*, *9*(4).

Tampubolon, W. S. (2016). Upaya Perlindungan Hukum Bagi Konsumen Ditinjau Dari Undang Undang Perlindungan Konsumen. *Jurnal Ilmiah Advokasi*, *4*(1), 53-61.

