PESHUM : Jurnal Pendidikan, Sosial dan Humaniora
Vol.5, No.5, Agustus 2026

Penegakan Hukum Pidana Terhadap Kejahatan Sniffing Berkedok Undangan Digital Berdasarkan UU ITE Dan UU PDP

Dimas Rezky Akbar[1] , Vicky Yohanes Posumah[2], Mohammad Reza Septiawan[3], Adithia Osea[4], Endang Suprapti[5]
[1,2,3,4,5] Universitas Tama Jagakarsa, Indonesia
E-mail: dimasrezkyakbar11@gmail.com[1], vicky.yohanes82@gmail.com[2], setiawanr57@gmail.com[3], adithiaosea9@gmail.com[4] , endangspt0@gmail.com[5]

Article History:
Received: 23 Juni 2026
Revised: 01 Agustus 2026
Accepted: 10 Agustus 2026

Keywords: *Sniffing; UU ITE; UU PDP; Mule Account; Pertanggungjawaban Korporasi.*

Abstract: *Transformasi perbankan digital di Indonesia diikuti oleh eskalasi kejahatan siber melalui modus rekayasa sosial berupa penyebaran Application Package File (APK) sniffing berkedok undangan digital. Penegakan hukum pidana saat ini seringkali mengalami kebuntuan akibat berlindungnya peretas di balik anonimitas lintas yurisdiksi dan penggunaan rekening penampung (mule account). Penelitian ini bertujuan menganalisis kualifikasi delik tindak pidana sniffing berdasarkan instrumen hukum positif serta merekonstruksi pertanggungjawaban hukum bagi penyelenggara sistem elektronik perbankan guna memutus rantai kejahatan tersebut. Penelitian ini menggunakan metode hukum yuridis normatif dengan pendekatan perundang-undangan (statute approach) dan konseptual (conceptual approach). Hasil penelitian menunjukkan bahwa, pertama, modus sniffing memenuhi unsur pidana akses ilegal, intersepsi, dan manipulasi sistem berdasarkan UU ITE, serta pencurian data keuangan yang diklasifikasikan sebagai data pribadi spesifik dalam UU PDP. Persetujuan korban atas instalasi aplikasi tidak menghapus unsur pidana karena dikualifikasikan sebagai cacat kehendak (vitiated consent). Kedua, kebuntuan yurisdiksi dapat diatasi dengan menerapkan pertanggungjawaban pidana korporasi dan doktrin tanggung jawab mutlak (strict liability) terhadap lembaga perbankan atas kelalaian pencegahan mule account. Otoritas Jasa Keuangan (OJK) perlu mereformulasi regulasi yang mewajibkan bank menerapkan Behavioral Know Your Customer (KYC) secara real-time.*

PENDAHULUAN

Transformasi digital di sektor perbankan Indonesia telah mengubah lanskap transaksi keuangan secara fundamental. Digitalisasi ini menawarkan efisiensi dan aksesibilitas tanpa batas bagi nasabah, ditandai dengan masifnya penggunaan layanan perbankan seluler (*mobile banking*).

Namun, pergeseran ekosistem transaksi dari konvensional menuju ruang siber membawa implikasi serius terhadap rentannya keamanan sistem informasi dan privasi data nasabah. Kejahatan siber di sektor perbankan tidak lagi hanya mengandalkan peretasan sistem secara teknis, tetapi telah berevolusi menggunakan rekayasa sosial (*social engineering*) yang mengeksploitasi kelengahan pengguna.

Sebagai bentuk *das sollen* atau kondisi ideal yang dicita-citakan oleh hukum positif, negara telah memberikan instrumen pelindungan normatif bagi nasabah. Pelindungan ini secara lex specialis diatur melalui Undang-Undang Nomor 11 Tahun 2008 yang telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) (Indonesia, 2024) , serta pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) (Indonesia, Undang Undang Indonesia tentang perlindungan Data Pribadi, UU No.27, LN No. 196, TLN No. 6820, 2022). Kedua instrumen hukum ini secara tegas mewajibkan Penyelenggara Sistem Elektronik (PSE), termasuk lembaga perbankan, untuk menjamin keandalan sistem elektronik dan menjaga kerahasiaan data pribadi nasabah dari akses yang tidak sah.

Namun, postulat hukum pelindungan tersebut berbenturan tajam dengan realitas empiris di lapangan. Alih-alih menyerang sistem keamanan berlapis milik bank, pelaku kejahatan kini mengeksploitasi celah psikologis nasabah melalui metode *sniffing*. Modus operandi ini dilakukan secara masif dengan mendistribusikan file berekstensi *Application Package File* (APK) berkedok undangan pernikahan digital atau tautan resi ekspedisi palsu. Saat file tersebut diunduh, perangkat lunak berbahaya (*malware*) bekerja di latar belakang sistem perangkat korban untuk meretas sistem *Short Message Service* (SMS) dan mencuri *One Time Password* (OTP) serta kredensial *mobile banking* tanpa disadari oleh korban.

Ketika nasabah yang menjadi korban melaporkan kerugian finansialnya, upaya penegakan hukum pidana oleh aparat seringkali berujung pada kebuntuan (*deadlock*). Investigasi siber kerap terhambat oleh dua kendala operasional yang krusial. Pertama, aliran dana hasil kejahatan dengan cepat diputus dan dialihkan melalui jaringan *mule account* (rekening penampung) yang dibuka menggunakan data identitas palsu atau identitas curian. Kedua, infrastruktur server pengendali utama yang dioperasikan oleh peretas acapkali berlokasi di luar yurisdiksi hukum Indonesia. Kondisi ini memperlihatkan adanya ketimpangan antara instrumen penegakan hukum konvensional yang berprinsip teritorial dengan karakteristik kejahatan siber yang bersifat nirkawasan (*borderless*) dan anonim.

Kajian mengenai kejahatan siber di sektor perbankan sejatinya telah banyak dilakukan oleh para sarjana hukum. Penelitian terdahulu, seperti yang dilakukan oleh Fitria Wulandari (2003), berfokus pada penerapan delik penipuan dan pencurian data dalam kerangka UU ITE secara umum. Senada dengan hal tersebut, Dianne Eka Rusmawati (2003) menelaah aspek pelindungan konsumen dengan menitikberatkan pada mekanisme ganti rugi perdata antara nasabah dan pihak bank ketika terjadi insiden pembobolan rekening. Sebagian besar literatur akademik yang ada saat ini cenderung menganalisis kejahatan *phishing* atau *sniffing* murni dari perspektif pertanggungjawaban individu pelaku (peretas), atau justru membebankan kerugian mutlak pada kelalaian nasabah selaku korban.

Meskipun demikian, kajian-kajian terdahulu tersebut masih menyisakan ruang kosong (*research gap*), terutama dalam menyikapi kebuntuan yurisdiksi penyidik dan maraknya pengalihan dana hasil kejahatan. Belum ada penelitian komprehensif yang secara spesifik mengkonstruksikan kelalaian sistemik bank dalam mendeteksi anomali *mule account* sebagai bentuk tindak pidana korporasi melalui pendekatan *strict liability*. Oleh karena itu, penelitian ini hadir untuk mengisi kekosongan literatur tersebut dengan mengintegrasikan rezim pemidanaan

UU ITE dan UU PDP, sekaligus merumuskan kewajiban *Behavioral KYC* sebagai standar kepatuhan hukum perbankan yang mutakhir.

Berdasarkan kesenjangan antara *das sollen* dan *das sein* tersebut, tulisan ini bertujuan untuk mengkaji secara komprehensif kualifikasi delik dan penegakan hukum pidana terhadap kejahatan *sniffing* berkedok undangan digital berdasarkan UU ITE dan UU PDP. Sebagai kebaruan (*novelty*) analisis, makalah ini akan menawarkan gagasan rekonseptualisasi pertanggungjawaban pidana korporasi bagi lembaga perbankan. Kelalaian perbankan dalam memitigasi pembukaan *mule account* akan ditinjau sebagai dasar mewajibkan pembaruan standar verifikasi *Know Your Customer* (KYC) digital, guna memutus ekosistem kejahatan perbankan digital dari akarnya.

METODE

Penelitian ini menggunakan metode penelitian hukum yuridis normatif, yaitu penelitian yang difokuskan pada pengkajian penerapan kaidah-kaidah atau norma-norma dalam hukum positif. Pendekatan masalah yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan dengan menelaah regulasi yang bersinggungan langsung dengan isu hukum yang diangkat, khususnya Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), serta regulasi terkait dari Otoritas Jasa Keuangan (OJK). Di sisi lain, pendekatan konseptual digunakan untuk membangun argumentasi hukum melalui doktrin dan pandangan para ahli, khususnya yang berkaitan dengan teori pertanggungjawaban pidana korporasi.

Sumber bahan hukum yang digunakan diklasifikasikan menjadi bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer terdiri dari peraturan perundang-undangan yang mengikat, sedangkan bahan hukum sekunder mencakup literatur hukum, buku, jurnal ilmiah, serta publikasi akademik lainnya yang relevan dengan kejahatan *sniffing* dan pelindungan data perbankan. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan menginventarisasi dokumen-dokumen hukum tersebut. Seluruh bahan hukum yang telah terkumpul dianalisis secara kualitatif normatif dan disajikan secara deskriptif analitis guna menjawab permasalahan terkait kebuntuan penegakan hukum dan rekonstruksi verifikasi *Know Your Customer* (KYC) secara komprehensif.

HASIL DAN PEMBAHASAN

Bagian ini menguraikan hasil analisis yuridis normatif mengenai dua isu hukum utama. Pertama, pembedahan kualifikasi delik dan pemenuhan unsur pidana dari modus *sniffing* melalui penyebaran APK berkedok undangan digital berdasarkan UU ITE dan UU PDP. Kedua, perumusan rekonseptualisasi pertanggungjawaban pidana korporasi bagi lembaga perbankan sebagai upaya komprehensif untuk menanggulangi menjamurnya rekening penampung (*mule account*).

1. Kualifikasi Delik dan Penegakan Hukum Pidana Modus *Sniffing*

Kejahatan *sniffing* melalui penyebaran *Application Package File* (APK) berkedok undangan digital atau resi kurir merupakan bentuk kejahatan siber kompleks yang memadukan rekayasa sosial (*social engineering*) dengan intrusi perangkat lunak berbahaya (*malware*). Secara doktrinal hukum pidana, perbuatan ini tidak dapat disederhanakan sekadar sebagai penipuan

konvensional (Pasal 378 KUHP), melainkan serangkaian tindak pidana siber yang melanggar ketentuan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Penegakan hukum pidana terhadap pelaku dapat dikonstruksikan melalui penerapan pasal berlapis (*concursus idealis*) dengan rincian kualifikasi delik sebagai berikut:

A. Akses Ilegal (*Illegal Access*) terhadap Sistem Perangkat Korban

Langkah pertama pelaku dalam mengelabui korban untuk mengunduh dan menginstal APK berbahaya memenuhi kualifikasi delik akses ilegal. Berdasarkan Pasal 30 ayat (1) jo. Pasal 46 ayat (1) UU ITE, setiap orang dilarang dengan sengaja dan tanpa hak atau melawan hukum mengakses Sistem Elektronik milik orang lain dengan cara apa pun. Meskipun korban secara teknis menekan tombol "setuju" (*allow*) saat menginstal APK, persetujuan tersebut dikategorikan sebagai cacat kehendak (*vitiated consent*) karena didapatkan melalui tipu muslihat. Aplikasi tersebut secara tersembunyi (*clandestine*) menerobos sistem keamanan (*security measure*) perangkat telepon seluler korban, yang secara mutlak melanggar hak privasi teritorial digital korban.

B. Intersepsi Ilegal (*Illegal Interception*) dan Manipulasi Data

Setelah APK terinstal, modus utama pelaku adalah mencuri kredensial perbankan dan *One Time Password* (OTP) yang dikirimkan oleh pihak bank melalui *Short Message Service* (SMS). Perbuatan ini secara sempurna memenuhi unsur delik Pasal 31 ayat (1) jo. Pasal 47 UU ITE terkait larangan melakukan intersepsi atau penyadapan atas informasi elektronik dalam suatu sistem yang tidak bersifat publik. *Malware* yang tertanam dalam APK tersebut dirancang untuk membaca, menyalin, dan meneruskan (mem-*forward*) setiap pesan masuk secara *real-time* ke server milik pelaku. Proses ini memfasilitasi pelaku untuk mengambil alih (*takeover*) akun perbankan korban dan melakukan transaksi finansial tanpa otorisasi.

C. Gangguan Sistem (*System Interference*)

Tindakan *malware* yang beroperasi di latar belakang (*background process*) acapkali memanipulasi sistem operasi perangkat korban, seperti menyembunyikan notifikasi SMS asli dari layar agar korban tidak menyadari adanya transaksi keluar. Modus ini dapat dijerat dengan delik gangguan sistem sebagaimana diatur dalam Pasal 33 jo. Pasal 49 UU ITE, yaitu tindakan yang berakibat sistem elektronik tidak bekerja sebagaimana mestinya.

Konstruksi pasal-pasal berlapis ini memberikan landasan yuridis yang tajam bagi penyidik Kepolisian untuk menindak pelaku pengirim APK tanpa harus menunggu pembuktian kerugian materiil di pihak perbankan, mengingat rumusan delik dalam UU ITE pada dasarnya merupakan delik formil yang menitikberatkan pada perbuatan terlarang itu sendiri.

D. Pencurian Data Keuangan sebagai Pelanggaran Data Pribadi Spesifik

Kredensial perbankan dan *One Time Password* (OTP) yang dicuri oleh pelaku bukan sekadar deretan angka acak, melainkan instrumen otentikasi yang memberikan akses langsung terhadap aset finansial korban. Dalam perspektif Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), informasi ini diklasifikasikan secara tegas sebagai "Data Pribadi yang Bersifat Spesifik", khususnya dalam kategori data keuangan pribadi sebagaimana diatur dalam Pasal 4 ayat (2) huruf c.

E. Pendekatan Doktrinal: *Mens Rea* dan Cacat Kehendak (*Vitiated Consent*)

Dalam menindak kejahatan *sniffing*, aparat penegak hukum seringkali dihadapkan pada dalil pembelaan pelaku yang mengklaim ketiadaan unsur paksaan. Pelaku berargumen bahwa korban secara sadar mengunduh aplikasi dan memberikan izin akses (*grant permission*) pada perangkatnya, sehingga tidak terjadi akses ilegal (*illegal access*). Secara doktrinal, argumentasi ini dapat dipatahkan menggunakan prinsip cacat kehendak (*vitiated consent*). Persetujuan yang

diberikan oleh korban merupakan persetujuan semu karena didapatkan melalui tipu muslihat (*bedrog*) dan penyesatan (*dwaling*). Niat jahat (*mens rea*) pelaku telah terwujud sejak awal proses rekayasa sosial, di mana mereka sengaja menyembunyikan sifat asli dari file APK tersebut. Oleh karena itu, interaksi korban tidak menghapus sifat melawan hukum dari perbuatan pelaku, melainkan justru menjadi bagian dari *actus reus* manipulasi sistem yang dirancang oleh pelaku.

F. Bedah Kasus: Penindakan Sindikat APK oleh Bareskrim Polri (2023)

Relevansi penerapan delik formil UU ITE dan pelindungan data spesifik dalam kasus *sniffing* dapat dilihat pada penindakan yang dilakukan oleh Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri pada awal tahun 2023. Dalam pengungkapan tersebut, kepolisian berhasil menangkap sindikat pembuat dan penyebar APK berkedok undangan pernikahan digital yang telah merugikan ratusan korban dengan estimasi kerugian mencapai belasan miliar rupiah.

Dalam proses penegakan hukumnya, penyidik secara tepat tidak menyederhanakan kasus ini menjadi delik penipuan konvensional (Pasal 378 KUHP). Para tersangka langsung dijerat dengan Pasal 46 ayat (1), (2), (3) jo. Pasal 30 ayat (1), (2), (3) UU ITE tentang akses ilegal, serta Pasal 48 ayat (1) jo. Pasal 32 ayat (1) UU ITE tentang modifikasi atau perusakan informasi elektronik. Tindakan tegas ini menjadi preseden hukum yang krusial. Penegakan hukum dalam kasus ini menegaskan bahwa distribusi *malware* berbasis rekayasa sosial merupakan bentuk kejahatan siber murni yang memicu rusaknya kerahasiaan data perbankan, sehingga pelakunya dapat dijerat hukuman maksimal tanpa perlu memperdebatkan tingkat kelalaian korban di awal kejadian.

Klasifikasi sebagai data spesifik ini berimplikasi pada pemberlakuan standar pelindungan dan ancaman sanksi yang lebih berat (*ultimum remedium*). Tindakan pelaku yang memanen data kredensial melalui APK *sniffing* memenuhi rumusan delik Pasal 65 ayat (1) jo. ayat (3) UU PDP, yakni secara melawan hukum memperoleh, mengumpulkan, dan menggunakan Data Pribadi yang bukan miliknya. Berdasarkan Pasal 67 UU PDP, perbuatan ini diancam dengan pidana penjara maksimal 5 (lima) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). Konstruksi hukum pemidanaan gabungan antara UU ITE dan UU PDP ini sejatinya telah memberikan pedang hukum yang tajam bagi aparat penegak hukum untuk memenjarakan pelaku secara maksimal. Namun, efektivitas pasal-pasal ini pada praktiknya lumpuh ketika dihadapkan pada realitas anonimitas siber dan jaringan *mule account* (rekening penampung) yang memfasilitasi pelarian aset korban.

2. Kebuntuan Yurisdiksi dan Rekonseptualisasi Pertanggungjawaban Pidana Korporasi Perbankan

Efektivitas penegakan hukum pidana terhadap kejahatan *sniffing* seringkali terhenti pada hambatan yurisdiksi dan anonimitas. Server pengendali *malware* yang berlokasi di luar yurisdiksi Indonesia menyulitkan penyidik kepolisian, mengingat hukum pidana nasional terikat pada asas teritorial. Selain itu, kecepatan aliran dana hasil kejahatan yang diputus melalui jaringan *mule account* (rekening penampung) membuat pengembalian aset korban (*asset recovery*) nyaris mustahil dilakukan secara konvensional.

Menghadapi kebuntuan yurisdiksi terhadap pelaku utama ini, orientasi penegakan hukum perlu diperluas dengan menyasar instrumen pemfasilitasi kejahatan tersebut, yakni kelemahan sistem perbankan. Maraknya *mule account* terjadi karena kegagalan sistem deteksi dini bank terhadap anomali transaksi. Rekening baru yang dioperasikan dengan data identitas palsu seringkali menunjukkan pola transaksi yang tidak wajar—seperti menerima dana dalam jumlah besar dan langsung mentransfernya habis ke puluhan rekening lain dalam hitungan menit (skema pencucian uang/ *layering*). Ketiadaan algoritma pemblokiran otomatis (*auto-block*) terhadap perilaku transaksi anomali ini merupakan bentuk kelalaian penyelenggara sistem elektronik.

Berdasarkan Peraturan Mahkamah Agung (Perma) Nomor 13 Tahun 2016 tentang Tata Cara Penanganan Perkara Tindak Pidana oleh Korporasi, lembaga perbankan dapat dimintai pertanggungjawaban pidana. Dalam Pasal 4 ayat (2) Perma tersebut, korporasi dapat dipidana apabila tidak melakukan langkah-langkah pencegahan, tidak mencegah dampak yang lebih besar, dan tidak memastikan kepatuhan terhadap ketentuan hukum yang berlaku. Kegagalan bank dalam mendeteksi dan memblokir anomali aliran dana hasil kejahatan *sniffing* secara *real-time* dapat dikonstruksikan sebagai pembiaran (kelalaian struktural) yang memfasilitasi terjadinya tindak pidana berlanjut.

Sebagai solusi komprehensif, perlu ada rekonseptualisasi kewajiban *Know Your Customer* (KYC) oleh Otoritas Jasa Keuangan (OJK). KYC tidak boleh lagi dipahami sekadar verifikasi dokumen identitas di awal pembukaan rekening (E-KYC), melainkan harus berevolusi menjadi *Behavioral* KYC dan *Continuous* KYC. Bank harus diwajibkan secara hukum untuk mengintegrasikan kecerdasan buatan (*Artificial Intelligence*) guna mendeteksi *liveness* pengguna dan memblokir anomali transaksi *mule account* secara *real-time*. Jika bank terbukti tidak memiliki atau tidak mengaktifkan standar keamanan mutakhir ini, aparat penegak hukum dapat menggunakan instrumen pertanggungjawaban pidana korporasi untuk menjatuhkan sanksi denda maksimal kepada bank, sekaligus mewajibkan bank mengganti kerugian finansial korban.

A. Pendekatan Doktrin *Strict Liability* terhadap Kelalaian Sistemik Bank

Dalam diskursus hukum pidana korporasi, ketiadaan niat jahat (*mens rea*) dari jajaran pengurus bank tidak serta-merta menghapus pertanggungjawaban pidana institusi. Kegagalan sistemik perbankan dalam mendeteksi dan memblokir *mule account* dapat dianalisis menggunakan doktrin *Strict Liability* (tanggung jawab mutlak). Berdasarkan doktrin ini, ketika sebuah korporasi menjalankan aktivitas yang memiliki risiko tinggi terhadap masyarakat—dalam hal ini menyelenggarakan lalu lintas finansial digital—korporasi tersebut secara otomatis memikul tanggung jawab pidana apabila risikonya mewujud menjadi kerugian publik, tanpa perlu membuktikan adanya unsur kesalahan (*fault*) atau niat jahat (Sjahdeini, 2017).

Penggunaan doktrin ini sangat relevan mengingat bank bertindak sebagai Pengendali Data dan Penyelenggara Sistem Elektronik (PSE). Jika algoritma keamanan bank terbukti gagal menyaring anomali pembukaan rekening baru yang secara masif digunakan untuk menampung aliran dana hasil *sniffing*, maka bank tersebut secara mutlak dianggap gagal memenuhi standar keandalan sistem. Penerapan *strict liability* akan memaksa perbankan untuk bergeser dari sekadar kepatuhan administratif (verifikasi KTP di awal) menuju kepatuhan proaktif, di mana bank wajib menanggung kerugian nasabah dan membayar denda pidana korporasi apabila sistem *Know Your Customer* (KYC) mereka berhasil ditembus oleh sindikat penipu.

B. Optimalisasi Peran Otoritas Jasa Keuangan (OJK) dalam Penegakan Kepatuhan

Penerapan pertanggungjawaban pidana korporasi dan doktrin *strict liability* harus diiringi dengan instrumen pengawasan yang lebih represif dari Otoritas Jasa Keuangan (OJK) selaku regulator sektor jasa keuangan. Saat ini, pedoman penyelenggaraan produk perbankan digital belum secara eksplisit mewajibkan bank untuk menghentikan transaksi secara sepihak berdasarkan deteksi anomali *real-time* dari sistem *Know Your Customer* (KYC). Oleh karena itu, OJK perlu merumuskan pembaruan regulasi yang mewajibkan setiap bank untuk memiliki sistem *Behavioral KYC*.

Sebagai instrumen penegak hukum administrasi, regulasi OJK tersebut harus memuat sanksi berjenjang yang tegas. Apabila sebuah bank terbukti melakukan pembiaran prosedural sehingga sistemnya memfasilitasi pembukaan jaringan *mule account* untuk kejahatan *sniffing*,

OJK dapat menjatuhkan sanksi administratif berupa pembekuan hingga pencabutan izin layanan perbankan digital (seperti aplikasi *mobile banking*) milik bank tersebut. Ancaman pencabutan izin ekosistem digital ini diyakini akan menjadi katalisator yang memaksa perbankan menggeser paradigma operasionalnya: dari sekadar mengejar target kuantitas pembukaan rekening baru, menuju jaminan perlindungan keamanan finansial nasabah secara mutlak.

KESIMPULAN

Berdasarkan analisis terhadap kualifikasi delik dan penegakan hukum kejahatan *sniffing* berkedok undangan digital, dapat ditarik dua kesimpulan utama:

1. **Kualifikasi Delik dan Penegakan Hukum Pidana:**

   Distribusi *Application Package File* (APK) berbahaya bukanlah penipuan konvensional, melainkan tindak pidana siber kompleks yang memenuhi jerat pasal berlapis. Perbuatan ini melanggar larangan akses ilegal, intersepsi ilegal, dan manipulasi sistem elektronik berdasarkan UU ITE, serta pencurian Data Pribadi Spesifik berupa kredensial keuangan berdasarkan UU PDP. Dalil pembelaan mengenai kelalaian korban yang menekan tombol persetujuan tidak dapat membatalkan unsur pidana, karena persetujuan tersebut masuk dalam kategori cacat kehendak (*vitiated consent*) akibat tipu muslihat rekayasa sosial (Hiariej, 2014).

2. **Rekonstruksi Pertanggungjawaban Pidana Korporasi:**

   Kebuntuan yurisdiksi dalam melacak pelaku utama dan aliran dana pada rekening penampung (*mule account*) dapat diurai dengan menyasar kelalaian sistemik lembaga perbankan. Melalui doktrin tanggung jawab mutlak (*strict liability*), perbankan dapat dimintai pertanggungjawaban pidana korporasi atas kegagalannya mendeteksi anomali transaksi. Untuk memutus ekosistem kejahatan ini, Otoritas Jasa Keuangan (OJK) harus mewajibkan transisi dari KYC konvensional menuju *Behavioral KYC* yang berkesinambungan, diiringi ancaman sanksi pencabutan izin layanan digital bagi bank yang tidak patuh.

DAFTAR PUSTAKA

Arief, B. N. (2006). *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. RajaGrafindo Persada.

Hiariej, E. O. S. (2014). *Prinsip-Prinsip Hukum Pidana*. Cahaya Atma Pustaka.

Sjahdeini, S. R. (2017). *Ajaran Pidana Korporasi: Sejarah, Konsep, dan Penerapannya*. Prenadamedia Group.

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

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Peraturan Mahkamah Agung Nomor 13 Tahun 2016 tentang Tata Cara Penanganan Perkara Tindak Pidana oleh Korporasi.