Abdi Implementasi Pancasila: Jurnal Pengabdian Masyarakat
p-ISSN XXXX-XXX, e-ISSN XXXX-XXXX

# UPAYA HUKUM PIDANA TERHADAP TINDAK PIDANA PENCURIAN KREDENSIAL DALAM TRANSAKSI MOBILE BANKING DI INDONESIA

Jason Gandirja

Program Studi Magister Ilmu Hukum Universitas Pancasila

Received : 12/07/2026
Revised : 18/08/2026
Accepted : 9/9/2026

*Corresponding author
Email : qpkjason@gmail.com

## Abstraksi

Peningkatan kejahatan siber pada layanan mobile banking menunjukkan pergeseran modus dari peretasan sistem menuju pencurian kredensial melalui rekayasa sosial, phishing, malware, dan eksploitasi celah API. Kondisi ini menimbulkan risiko serius bagi keamanan transaksi digital dan menuntut evaluasi terhadap efektivitas kerangka hukum pidana yang berlaku. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus untuk menganalisis kecukupan norma pidana dalam UU ITE dan KUHP serta pertanggungjawaban pelaku, termasuk kemungkinan penerapan asas ekstrateritorial Pasal 2 UU ITE. Hasil penelitian menunjukkan bahwa meskipun kerangka hukum telah tersedia, efektivitas penegakannya masih rendah akibat kendala teknis pembuktian digital, kelemahan pengawasan pihak ketiga, serta belum adanya pedoman khusus penanganan credential stealing. Penelitian ini menegaskan perlunya penguatan kapasitas aparat, pembaruan kebijakan keamanan siber, dan peningkatan literasi digital masyarakat.

*Kata kunci:* pencurian kredensial, hukum pidana siber, mobile banking.

## Abstract

The rise of cybercrime targeting mobile banking services indicates a shift in modus operandi from system intrusion to credential theft through social engineering, phishing, malware, and the exploitation of API vulnerabilities. This development poses significant risks to the security of digital financial transactions and necessitates an evaluation of the effectiveness of the existing criminal law framework. This study employs a normative juridical method using statutory, conceptual, and case approaches to analyze the adequacy of criminal provisions in the Electronic Information and Transactions Act (UU ITE) and the Criminal Code (KUHP), as well as the criminal liability of offenders, including the application of the extraterritorial principle under Article 2 of the UU ITE. The findings reveal that although a legal framework exists, its enforcement remains weak due to technical challenges in digital evidence, insufficient oversight of third parties, and the absence of specific guidelines for handling credential theft. This study emphasizes the need to strengthen investigative capacity, update cybersecurity policies, and enhance public digital literacy.

*Keywords:* credential theft, cyber criminal law, mobile banking.

© 2026 Penerbit LPPM UP. All rights reserved

## PENDAHULUAN

Perkembangan teknologi informasi dalam satu dekade terakhir telah mendorong transformasi signifikan dalam sektor keuangan Indonesia, termasuk meningkatnya adopsi layanan mobile banking sebagai sarana utama transaksi digital masyarakat. Kemudahan, kecepatan, dan efisiensi yang ditawarkan membuat mobile banking menjadi bagian penting dalam sistem pembayaran nasional. Namun, modernisasi ini juga menciptakan ruang serangan baru bagi pelaku kejahatan siber yang semakin adaptif dan kompleks. Pergeseran pola serangan dari system breach menuju pencurian kredensial (credential stealing) berbasis rekayasa sosial, malware, dan eksploitasi celah integrasi sistem pihak ketiga menunjukkan bahwa ancaman kejahatan digital kini tidak hanya bersifat teknis, melainkan menyasar titik terlemah dalam ekosistem perbankan, yaitu pengguna serta pengamanan antarmuka sistem yang tidak memadai.

Dalam kerangka das sollen, perlindungan data elektronik dan keamanan transaksi digital telah dijamin melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan UU Nomor 19 Tahun 2016 (UU ITE). Pasal 30 ayat (1)–(3) melarang akses ilegal terhadap sistem elektronik, sedangkan Pasal 32 ayat (1) melarang perolehan, perubahan, atau pengalihan data tanpa hak. Ketentuan pidananya diatur dalam Pasal 46 dan Pasal 48 UU ITE. Selain itu, tindakan pencurian dana melalui kredensial yang dicuri dapat dikualifikasikan sebagai tindak pidana pencurian menurut Pasal 362 KUHP atau penipuan menurut Pasal 378 KUHP. Secara normatif, sistem hukum Indonesia telah menyiapkan perangkat hukum yang cukup memadai untuk

© 2026 Segala bentuk plagiarisme dan penyalahgunaan hak kekayaan intelektual akibat diterbitkannya paper pengabdian masyarakat ini sepenuhnya menjadi tanggung jawab penulis.

melindungi transaksi electronica. Namun, pada tataran das sein, sejumlah insiden sepanjang 2025 menunjukkan bahwa sistem pengamanan dan penegakan hukumnya belum mampu mengimbangi kecepatan inovasi pelaku kejahatan siber. Kasus pembobolan Rekening Dana Nasabah (RDN) PT Panca Global Sekuritas mengungkap kelemahan serius pada Application Programming Interface (API) yang tidak dilengkapi mekanisme OTP atau TFA. Serangkaian transfer ke rekening non-whitelist dapat terjadi tanpa terdeteksi, sebagaimana disampaikan oleh pakar keamanan digital Alfons Tanujaya dan Heru Sutadi (Fikaz 2025). Insiden ini menegaskan bahwa pelaku tidak perlu meretas sistem inti bank untuk melakukan kejahatan, melainkan cukup mengeksploitasi celah keamanan pihak ketiga.

Selain itu, malware generasi baru seperti Ghofirin(Ghofirin 2025)memperlihatkan kemajuan signifikan dalam pola serangan berbasis kredensial. Malware ini menyamar sebagai aplikasi sah dan meminta akses ke fitur accessibility service sehingga dapat merekam layar, membaca notifikasi, mencatat tombol ketikan, dan mengambil alih akun mobile banking secara penuh. Laporan Kaspersky yang dikutip CNBC Indonesia menunjukkan lebih dari 1.250 korban sejak pemantauan dilakukan (Redaksi 2025). Masifnya instalasi APK dari luar toko resmi, ditambah rendahnya literasi digital masyarakat, memperbesar risiko keberhasilan serangan.

Tidak hanya pencurian kredensial, sektor keuangan juga menghadapi ancaman serius melalui serangan ransomware. Insiden LockBit yang menimpa Bank Syariah Indonesia (BSI) memperlihatkan bahwa pelaku memanfaatkan teknologi enkripsi, mata uang kripto, dan jaringan anonim TOR untuk menghilangkan jejak, sehingga menyulitkan proses investigasi oleh aparat penegak hukum (Ghofirin, 2025). Kejadian ini menunjukkan bahwa cakupan ancaman tidak hanya terkait pencurian data akses pengguna, tetapi juga upaya sabotase sistem perbankan secara sistematis. Ketiga kasus tersebut API yang dieksploitasi (Fikaz 2025), malware Zanubis (Redaksi 2025), dan ransomware pada BSI (Ghofirin 2025) menggambarkan bahwa ekosistem mobile banking berada dalam titik krusial. Di satu sisi, mobile banking sangat penting untuk mendukung sistem pembayaran nasional. Di sisi lain, lemahnya perlindungan kredensial menempatkan pengguna dan lembaga keuangan dalam posisi rentan, sehingga membutuhkan intervensi hukum pidana yang lebih kuat dan adaptif.

Berdasarkan kondisi tersebut, kajian mengenai upaya hukum pidana dalam menanggulangi pencurian kredensial pada transaksi mobile banking menjadi sangat relevan. Permasalahan yang muncul meliputi:

1. efektivitas regulasi dalam menghadapi modus kejahatan baru yang menggabungkan rekayasa sosial, malware, dan eksploitasi API;
2. kesulitan pembuktian unsur pidana karena penggunaan teknologi penyamaran;
3. belum optimalnya koordinasi antara bank, OJK, dan aparat penegak hukum; serta
4. minimnya pedoman teknis mengenai penanganan kasus credential stealing.

Dengan demikian, penelitian ini perlu dilakukan untuk menganalisis perkembangan modus pencurian kredensial, efektivitas penegakan hukum pidana yang berlaku, pertanggungjawaban pelaku termasuk ruang lingkup asas ekstrateritorial Pasal 2 UU ITE, serta strategi pencegahan melalui pembaruan regulasi dan penguatan kapasitas teknis aparat. Penelitian ini menegaskan bahwa perlindungan pengguna mobile banking membutuhkan kebijakan penegakan hukum yang adaptif, responsif, dan kolaboratif agar keamanan sistem perbankan nasional dan kepercayaan publik terhadap layanan digital tetap terjaga.

## METODE PELAKSANAAN

Penelitian ini menggunakan metode yuridis normatif yang bertumpu pada analisis terhadap peraturan perundang-undangan, asas hukum, dan doktrin yang relevan dengan tindak pidana pencurian kredensial dalam transaksi mobile banking. Kajian dilakukan melalui pendekatan perundang-undangan (statute approach) terhadap ketentuan dalam UU ITE, KUHP, serta regulasi perbankan terkait keamanan digital; pendekatan konseptual (conceptual approach) untuk memahami konstruksi pertanggungjawaban pidana dan karakteristik kejahatan siber; serta pendekatan kasus (case approach) yang menelaah insiden aktual seperti pembobolan RDN, malware (Redaksi 2025), dan ransomware pada institusi perbankan. Seluruh data sekunder berupa literatur ilmiah, jurnal, buku, regulasi, serta laporan media dianalisis menggunakan teknik deskriptif kualitatif, sehingga menghasilkan pemetaan mendalam mengenai kesenjangan antara pengaturan normatif (das sollen) dan kondisi empiris (das sein), serta merumuskan rekomendasi penguatan upaya hukum pidana dalam menghadapi kejahatan credential stealing.

## PEMBAHASAN

### Modus Operandi Tindak Pencurian Kredensial Mobile Banking Tahun 2025

Pergeseran modus kejahatan siber pada tahun 2025 menunjukkan transformasi signifikan dalam orientasi serangan pelaku, yang tidak lagi berfokus pada peretasan sistem inti perbankan (system breach), tetapi pada pencurian kredensial (credential

stealing) sebagai titik paling rentan dalam ekosistem keamanan digital(Rianda 2025). Kejahatan ini memanfaatkan kerentanan manusia melalui rekayasa sosial dan manipulasi perilaku pengguna, sehingga pelaku dapat memperoleh akses langsung ke akun mobile banking tanpa perlu menembus sistem perbankan yang memiliki lapisan keamanan lebih kuat. Pola ini menunjukkan bahwa strategi kejahatan siber kontemporer bergerak dari pendekatan teknis menuju pendekatan psikologis dan operasional, dengan memanfaatkan faktor kelengahan pengguna serta integrasi sistem pihak ketiga yang tidak aman. Pergeseran ini memperlihatkan bahwa pelaku semakin adaptif dan berorientasi pada jalur serangan yang memberikan hasil cepat dengan risiko rendah(Mulianingsih, Fajar, and Suharyati 2025).

Kasus pembobolan Rekening Dana Nasabah (RDN) PT Panca Global Sekuritas menjadi bukti nyata bahwa titik kritis keamanan bukan lagi pada sistem perbankan, melainkan pada keamanan Application Programming Interface (API) pihak ketiga yang terhubung ke sistem bank. API yang tidak dilengkapi lapisan verifikasi seperti One-Time Password (OTP) atau Two-Factor Authentication (TFA) menjadi celah utama yang memungkinkan pelaku memindahkan dana ke rekening non-whitelist secara berulang tanpa terdeteksi(Fikaz 2025). Peristiwa ini mengindikasikan bahwa kejahatan tidak dilakukan dengan meretas bank, tetapi mengeksploitasi kelalaian prosedural dan lemahnya pengawasan internal. Hal ini sejalan dengan ketentuan compliance sektor keuangan, yang sejatinya menuntut pengamanan berlapis dan audit berkala terhadap sistem pihak ketiga, meskipun tidak diatur secara spesifik dalam UU namun menjadi bagian dari prinsip kehati-hatian dalam industri perbankan.

Modus serangan yang bersandar pada rekayasa sosial sering kali memanfaatkan ketidaksiapan pengguna dalam mengidentifikasi upaya penipuan. Teknik phishing melalui tautan palsu, pesan pendek, maupun panggilan telepon dengan penyamaran identitas, memberikan kesempatan bagi pelaku untuk mengumpulkan data kredensial secara langsung dari korban. Metode ini semakin berbahaya karena pelaku memanfaatkan teknik manipulatif yang meniru komunikasi resmi bank, sehingga korban tidak menyadari bahwa informasi yang diberikan membuka akses bagi pelaku ke akun mobile banking(Mukhra et al. 2024). Secara hukum, tindakan memperoleh informasi elektronik secara melawan hukum merupakan pelanggaran terhadap Pasal 32 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan UU No. 19 Tahun 2016, yang melarang perolehan, pengubahan, dan pengalihan informasi elektronik tanpa hak.

Selain rekayasa sosial, evolusi malware menjadi faktor yang mempercepat terjadinya pencurian kredensial. Malware Zanubis (Redaksi 2025) merupakan contoh paling relevan, karena mampu menyamar sebagai aplikasi legal dan memperoleh hak akses melalui accessibility service pada perangkat Android. Malware ini dapat melakukan perekaman layar, keylogging, membaca notifikasi, hingga mengambil alih fungsi perangkat secara penuh. Dengan kontrol sebesar ini, pelaku seolah-olah dapat mengakses mobile banking korban seperti pemilik sah, sehingga sangat sulit bagi sistem bank mendeteksi transaksi mencurigakan(Redaksi 2025). Aksi pengambilan data ini dapat dikualifikasikan sebagai pelanggaran terhadap Pasal 30 ayat (1), (2), dan (3) UU ITE, yang mengatur larangan akses tanpa hak ke sistem elektronik, serta terhadap Pasal 46 UU ITE yang memberikan ancaman pidana atas tindakan tersebut.

Distribusi malware melalui file APK di luar toko aplikasi resmi menjadi jalur penyebaran yang sangat efektif. Pelaku sering menyamar sebagai institusi yang memiliki kredibilitas tinggi, seperti lembaga pemerintah, perusahaan energi, atau bahkan bank(Rizqullah et al. 2025). Pengguna yang tidak memahami struktur keamanan aplikasi dengan mudah tertipu karena tampilan antarmuka aplikasi palsu dibuat menyerupai aplikasi resmi. Ketika pengguna memberikan izin akses, malware mulai mengumpulkan data kredensial perbankan dan sandi perangkat. Aktivitas ini memperlihatkan bahwa faktor human error menjadi elemen utama keberhasilan pelaku, bukan kemampuan teknis tingkat tinggi. Secara normatif, tindakan ini dapat dikategorikan sebagai perbuatan mengambil data secara melawan hukum yang melanggar Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE.

Eksploitasi kelemahan API oleh pelaku kejahatan dalam kasus RDN juga menunjukkan bahwa koordinasi antara lembaga keuangan dan sistem keamanan digital belum optimal. API menjadi penghubung antara sistem sekuritas dan bank, namun ketika pengamanan tidak mengikuti standar verifikasi multi-faktor, API menjadi target mudah bagi pelaku yang telah menguasai kredensial. Selain itu, kegagalan pengawasan transaksi secara real-time memberikan ruang bagi pelaku untuk melakukan transaksi berulang dalam waktu singkat. Aktivitas ini, jika ditemukan adanya kelalaian atau pembiaran internal, dapat pula berkaitan dengan isu pertanggungjawaban pidana korporasi sesuai prinsip yang berkembang dalam hukum pidana modern dan diakui dalam konteks kejahatan siber(Putra, Abdurrachman, and Hamzani 2023).

Secara keseluruhan, pencurian kredensial juga berkaitan dengan perbuatan mengambil harta orang lain secara melawan hukum sebagaimana diatur dalam Pasal 362 Kitab Undang-Undang Hukum

Pidana (KUHP) tentang pencurian. Dalam konteks mobile banking, tindakan memindahkan dana dari rekening korban ke rekening lain menggunakan kredensial yang dicuri dapat dikualifikasikan sebagai pencurian karena memenuhi unsur mengambil barang (dana) yang seluruhnya atau sebagian milik orang lain. Apabila dilakukan melalui tipu muslihat, penyalahgunaan kepercayaan, atau rangkaian kebohongan, tindakan tersebut juga dapat memenuhi unsur Pasal 378 KUHP tentang penipuan. Dengan demikian, modus operandi pencurian kredensial tidak hanya merupakan pelanggaran terhadap UU ITE, tetapi juga termasuk tindak pidana konvensional dalam ranah KUHP.

**Efektivitas Sanksi Pidana dan Penegakan Hukum dalam Menanggulangi Credential Stealing**

**1. Efektivitas Sanksi Pidana dalam Kerangka Regulasi yang Ada**

Efektivitas sanksi pidana terhadap tindak pidana pencurian kredensial dalam transaksi mobile banking sangat ditentukan oleh kecukupan norma hukum positif yang berlaku. Regulasi mengenai kejahatan ini pada dasarnya telah diatur secara komprehensif dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (UU ITE). Ketentuan Pasal 30 ayat (1), (2), dan (3) UU ITE menegaskan larangan bagi setiap orang yang mengakses sistem elektronik milik orang lain tanpa hak, dengan ancaman pidana sebagaimana diatur dalam Pasal 46 ayat (1), (2), dan (3) UU ITE. Selain itu, tindakan memperoleh, menyalin, atau mentransmisikan informasi elektronik secara melawan hukum diatur dalam Pasal 32 ayat (1) UU ITE, yang dikenakan sanksi pidana berdasarkan Pasal 48 ayat (1) UU ITE. Kerangka pidana ini sesungguhnya cukup untuk mengkualifikasikan tindakan pencurian kredensial sebagai tindak pidana yang dapat ditindak secara tegas.

Meski demikian, efektivitas sanksi pidana tersebut belum optimal karena karakter kejahatan siber yang bersifat dinamis dan terus berkembang(Nainggolan 2025). Salah satu hambatan yang muncul adalah kemampuan pelaku untuk memanfaatkan teknologi mutakhir seperti malware, keylogger, dan phishing engine yang dapat berjalan otomatis tanpa intervensi langsung dari pelaku di setiap tahap kejahatan. Hal ini menyulitkan penegak hukum dalam membuktikan unsur kesengajaan (mens rea) sebagaimana dipersyaratkan dalam hukum pidana. Ketika kejahatan dijalankan melalui sistem otomatis atau skrip yang berjalan secara mandiri, pertanyaan mengenai intensi pelaku menjadi semakin kompleks dan sering kali menghambat proses penegakan hukum(Budiyanto and others 2025). Selain ketentuan dalam UU ITE, tindakan memindahkan dana dari rekening nasabah ke rekening lain menggunakan kredensial yang dicuri juga dapat dikualifikasikan sebagai tindak pidana pencurian sebagaimana diatur dalam Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP). Apabila perbuatan tersebut dilakukan melalui tipu muslihat, penyalahgunaan kepercayaan, atau rangkaian kebohongan, maka dapat pula dijerat dengan Pasal 378 KUHP tentang penipuan. Namun, penerapan pasal-pasal KUHP ini juga menghadapi tantangan, terutama karena KUHP dirancang untuk kejahatan konvensional sehingga tidak sepenuhnya mengakomodasi bentuk dan karakteristik kejahatan siber yang melibatkan perantara teknologi.

Hambatan lain ditemukan dalam kasus serangan digital yang melibatkan ransomware seperti insiden pada Bank Syariah Indonesia (BSI)(Ghofirin 2025). Serangan tersebut menggunakan teknologi enkripsi tingkat tinggi, jaringan anonim The Onion Router (TOR), dan mata uang kripto yang membuat pelacakan aliran dana dan identitas pelaku menjadi sangat sulit. Dalam konteks ini, sanksi pidana yang tersedia dalam UU ITE tetap relevan, namun efektivitasnya bergantung pada kemampuan aparat dalam melacak bukti digital yang sering kali terfragmentasi, terenskripsi, atau berada di luar yurisdiksi Indonesia.

**2. Tantangan Penegakan Hukum dan Kebutuhan Pembaruan Kebijakan**

Tantangan utama dalam penegakan hukum terkait pencurian kredensial adalah keterbatasan kapasitas investigasi di bidang forensik digital. Kejahatan siber yang memanfaatkan malware otomatis, eksploitasi API, dan rekayasa sosial lintas platform membutuhkan keahlian teknis yang tidak selalu dimiliki oleh aparat penegak hukum di tingkat penyidikan(Indradjaja, Suseno, and Atmaja 2024). Ketika alat bukti digital tidak ditangani dengan metode forensik yang tepat, validitasnya dapat diragukan di persidangan, sehingga efektivitas penegakan hukum semakin menurun. Kondisi ini menunjukkan perlunya peningkatan kompetensi teknis penyidik dalam bidang cyber forensics, log analysis, dan penelusuran jejak digital lintas jaringan. Selain persoalan teknis, yurisdiksi lintas negara juga menjadi hambatan serius dalam proses penegakan hukum. Pelaku kejahatan siber kerap beroperasi dari luar negeri dengan memanfaatkan infrastruktur server, layanan cloud, atau VPN yang berlokasi di berbagai negara. Sementara itu, UU ITE hanya memberikan dasar penerapan yurisdiksi berdasarkan Pasal 2 UU ITE, yaitu ketika perbuatan memiliki akibat hukum di wilayah Indonesia. Namun, dalam praktiknya, kerja sama internasional sering memerlukan prosedur yang panjang dan kompleks, sehingga penyidikan sering kali tidak menghasilkan

penangkapan pelaku meskipun norma pidana telah tersedia.

Problem lain yang turut melemahkan efektivitas penegakan hukum adalah minimnya audit keamanan mandiri terhadap mitra bank, terutama pada aspek integrasi API dan prosedur autentikasi. Kasus pembobolan RDN PT Panca Global Sekuritas menunjukkan kelemahan dalam pengamanan API yang tidak dilengkapi OTP/TFA. Padahal, bank telah menerapkan standar keamanan yang lebih ketat pada layanan internal seperti token atau sistem autentikasi berlapis(Farahdiva, Mulyana, and Asri 2025). Situasi ini memperlihatkan adanya kesenjangan regulasi dalam mengatur tanggung jawab pihak ketiga dalam ekosistem perbankan digital. Kelemahan lain adalah absennya pedoman operasional baku (SOP) atau guideline nasional yang secara khusus mengatur penanganan tindak pidana credential stealing pada layanan mobile banking. Tanpa adanya pedoman yang jelas, penegak hukum sering kali menunda proses penyidikan karena ketidakpastian prosedural, terutama dalam pengamanan bukti digital dan koordinasi dengan lembaga perbankan(Rinaldi and Wijaya 2025). Hal ini menyebabkan penegakan hukum berjalan lambat dan tidak efektif, meskipun norma pidana telah tersedia.

Oleh sebab itu, meskipun kerangka normatif mengenai kejahatan pencurian kredensial telah tersedia secara cukup melalui UU ITE dan KUHP, efektivitas penerapannya dalam praktik masih memerlukan pembaruan kebijakan, peningkatan kapasitas investigasi, penguatan kerja sama lintas lembaga, serta pembentukan pedoman teknis penanganan kejahatan siber. Tanpa langkah-langkah tersebut, sanksi pidana yang telah disediakan oleh undang-undang tidak akan mampu memberikan efek jera secara optimal maupun melindungi masyarakat dari ancaman pencurian kredensial yang semakin canggih dan adaptif.

**Pertanggungjawaban Pidana Pelaku Pencurian Kredensial dalam Mobile Banking**

**1. Pertanggungjawaban Pidana Individu Pelaku Kejahatan Pencurian Kredensial**

Pertanggungjawaban pidana terhadap pelaku pencurian kredensial dalam transaksi mobile banking harus dianalisis berdasarkan konstruksi hukum pidana positif yang berlaku di Indonesia. Pelaku yang secara sengaja mengakses sistem elektronik milik orang lain tanpa hak dapat dikenakan ketentuan Pasal 30 ayat (1), (2), dan (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah dengan UU Nomor 19 Tahun 2016, yang mengatur larangan akses ilegal, penguasaan sistem, serta peretasan akun. Ancaman pidananya diatur dalam Pasal 46 ayat (1), (2), dan (3) UU ITE, yang memberikan hukuman maksimal hingga 8 tahun penjara, tergantung derajat pelanggaran yang dilakukan terhadap sistem elektronik korban. Selain akses ilegal, pelaku yang memperoleh, menyalin, mentransmisikan, atau menyebarkan data kredensial perbankan secara tidak sah dapat dijerat berdasarkan Pasal 32 ayat (1) UU ITE, yang melarang setiap orang dengan sengaja dan tanpa hak mengubah, menambah, mengurangi, mentransfer, mengalihkan, atau merusak informasi elektronik milik orang lain. Sanksi pidananya tercantum dalam Pasal 48 ayat (1) UU ITE, dengan ancaman pidana penjara maksimal 8 tahun dan/atau denda hingga Rp2 miliar. Ketentuan ini relevan diterapkan pada pelaku malware yang mengambil data login, OTP, atau PIN korban melalui keylogging, screen recording, maupun teknik manipulasi izin akses aplikasi.

Jika pencurian kredensial mengakibatkan pemindahan dana secara melawan hukum, maka pertanggungjawaban pidana dapat diperluas kepada ketentuan Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP) yang mengatur tindak pidana pencurian, yaitu mengambil barang milik orang lain dengan melawan hukum. Dana elektronik yang dipindahkan dari rekening korban ke rekening pelaku atau pihak lain dapat dikualifikasikan sebagai "barang" dalam konteks pencurian(Pakpahan et al. 2023). Selain itu, untuk modus berbasis rekayasa sosial seperti phishing, yang mengandalkan tipu muslihat, penyalahgunaan kepercayaan, atau kebohongan sistematis, pelaku dapat dijerat dengan Pasal 378 KUHP tentang penipuan. Kedua pasal ini melengkapi rezim pertanggungjawaban pidana dalam KUHP yang masih relevan digunakan pada kejahatan siber modern.

Dalam kasus serangan berbasis malware yang lebih canggih, seperti CNN (Redaksi 2025) yang mampu mengambil alih perangkat korban melalui izin accessibility service, pertanggungjawaban pidana dapat meluas kepada pembuatan atau pendistribusian program berbahaya. Meskipun UU ITE tidak secara eksplisit menyebutkan istilah "malware", tindakan menciptakan atau menyebarkan program yang merusak atau mengganggu sistem elektronik dapat dikategorikan sebagai perbuatan melawan hukum berdasarkan Pasal 30 jo. Pasal 46 UU ITE, karena malware tersebut pada hakikatnya digunakan untuk mengakses dan mengendalikan sistem elektronik tanpa hak. Dalam doktrin hukum pidana siber, tindakan ini dikualifikasikan sebagai unlawful interference terhadap perangkat digital korban. Aspek yurisdiksi juga menjadi elemen penting dalam pertanggungjawaban pidana pelaku pencurian kredensial. Pelaku kejahatan siber sering kali beroperasi dari luar negeri dengan memanfaatkan jaringan anonim (TOR), server asing, atau mata uang kripto. Namun, berdasarkan Pasal 2

UU ITE, yurisdiksi pidana Indonesia tetap berlaku apabila perbuatan tersebut menimbulkan akibat hukum di Indonesia atau melibatkan sistem elektronik yang berada di wilayah hukum Indonesia. Artinya, meskipun pelaku tidak berada secara fisik di Indonesia, pertanggungjawaban pidana tetap dapat diterapkan sepanjang kejahatan tersebut menimbulkan kerugian bagi warga negara Indonesia atau entitas hukum yang berada dalam yurisdiksi Indonesia.

**2. Pertanggungjawaban Korporasi dan Pihak Ketiga dalam Ekosistem Keamanan Perbankan Digital**

Selain pertanggungjawaban individu, kejahatan pencurian kredensial dalam mobile banking sering kali berkaitan dengan kelalaian atau kelemahan prosedural pada pihak ketiga, seperti perusahaan sekuritas atau penyedia layanan API. Dalam kasus pembobolan Rekening Dana Nasabah PT Panca Global Sekuritas, misalnya, celah keamanan API tanpa autentikasi berlapis (OTP/TFA) membuka peluang bagi pelaku untuk mengeksploitasi transaksi keuangan. Apabila terbukti bahwa kelalaian pengawasan, kurangnya audit keamanan, atau pembiaran prosedural menjadi faktor penyebab terjadinya kejahatan, maka pertanggungjawaban pidana korporasi dapat diterapkan berdasarkan prinsip strict liability atau vicarious liability yang telah diakui dalam perkembangan hukum pidana modern. Dalam konteks hukum positif Indonesia, meskipun KUHP belum mengatur secara eksplisit pertanggungjawaban pidana korporasi untuk kejahatan siber, berbagai undang-undang sektoral seperti UU ITE dan UU Perbankan memberikan ruang untuk menilai kesalahan lembaga yang lalai dalam menerapkan standar keamanan sistem elektronik(Bahri 2023). UU ITE mengatur bahwa penyelenggara sistem elektronik wajib menyelenggarakan sistem elektronik secara andal, aman, dan bertanggung jawab. Apabila kegagalan keamanan berasal dari kelalaian penyelenggara sistem elektronik, maka entitas tersebut dapat dimintai pertanggungjawaban, baik secara perdata maupun administratif, dan dalam kondisi tertentu dapat dikualifikasikan masuk ke ranah pidana apabila terjadi pembiaran (omission) yang disengaja.

Pertanggungjawaban korporasi semakin relevan dalam konteks pencurian kredensial karena sebagian besar transaksi mobile banking melibatkan integrasi berbagai sistem elektronik yang saling terhubung(Risko and Krisnadi 2025). Ketika salah satu titik dalam rantai sistem tersebut tidak memenuhi standar keamanan, risiko kejahatan meningkat secara eksponensial. Dalam teori hukum pidana korporasi, entitas dianggap dapat dipidana apabila perbuatan pidana dilakukan oleh pengurus yang bertindak dalam lingkup tugas, atau apabila korporasi mendapatkan manfaat dari tindakan tersebut. Dalam konteks kejahatan kredensial, kelalaian institusi dalam mengamankan API atau sistem autentikasi dapat dianggap sebagai bentuk kesalahan struktural (organizational fault). Selain itu, pertanggungjawaban dapat diperluas kepada pihak-pihak yang ikut menyebabkan terjadinya kejahatan, baik secara sengaja maupun karena kelalaian berat (gross negligence)(Sadzili and Abubakar 2025). Apabila penyedia layanan teknologi atau pihak sekuritas tidak melakukan pembaruan keamanan, mengabaikan peringatan teknis, atau tidak menerapkan standar autentikasi yang diwajibkan oleh regulasi perbankan, maka tindakan tersebut dapat dikualifikasikan sebagai pembiaran yang dapat berkonsekuensi pidana. Dalam beberapa kasus, lembaga pengawas seperti Otoritas Jasa Keuangan (OJK) dapat merekomendasikan penegakan hukum terhadap institusi yang dianggap lalai menjaga keamanan data nasabah.

Dengan demikian, pertanggungjawaban pidana pelaku pencurian kredensial dalam mobile banking tidak hanya difokuskan pada individu pelaku, melainkan juga harus mempertimbangkan tanggung jawab sistemik dalam ekosistem keamanan digital. Pendekatan ini sejalan dengan kebutuhan untuk memperkuat integritas dan keamanan sistem keuangan nasional, terutama di tengah meningkatnya kompleksitas kejahatan siber yang melibatkan teknologi canggih dan jaringan lintas negara.

**Upaya Pencegahan dan Strategi Hukum Pidana Menghadapi Pergeseran Taktik Cybercrime**

Upaya pencegahan dan strategi hukum pidana menghadapi kejahatan pencurian kredensial dalam mobile banking harus dirancang secara komprehensif dan berorientasi pada mitigasi risiko sebelum kejahatan terjadi. Pergeseran taktik pelaku dari system breach menuju credential stealing menunjukkan bahwa titik serangan kini lebih banyak diarahkan pada pengguna, sistem integrasi pihak ketiga, serta kelemahan autentikasi(Santoso 2023). Oleh karena itu, strategi hukum pidana yang sebelumnya berfokus pada penindakan harus diperluas menjadi pendekatan preventif yang mencakup penguatan regulasi, peningkatan infrastruktur teknologi, dan edukasi publik. Pendekatan ini sejalan dengan asas ultimum remedium dalam hukum pidana, yang menempatkan pencegahan sebagai prioritas utama agar penegakan hukum tidak hanya bersifat represif tetapi juga proaktif dalam meminimalisasi risiko kejahatan digital(Saputri and Sulastri 2025).

Penegak hukum memegang peran strategis dalam upaya pencegahan tersebut, terutama melalui

peningkatan kapasitas digital forensik dan kompetensi teknis penyidik. Kejahatan pencurian kredensial sering kali dilakukan melalui malware, bot otomatis, dan rekayasa sosial lintas platform, sehingga pembuktian unsur kesengajaan dan pelacakan jejak digital memerlukan perangkat forensik yang canggih(Wibowo, Wangsajaya, and Surahmat 2023). Tanpa peningkatan kemampuan teknis aparat, sanksi pidana dalam Pasal 30 jo. Pasal 46 UU ITE dan Pasal 32 jo. Pasal 48 UU ITE akan sulit diterapkan secara efektif. Oleh karena itu, reformasi struktural pada lembaga penegak hukum diperlukan, termasuk pembaruan Standard Operating Procedure (SOP) penanganan kejahatan siber agar selaras dengan modus kejahatan kredensial yang terus berevolusi. Di samping aspek teknis, perlu adanya pedoman penegakan hukum yang secara khusus mengatur prosedur identifikasi, pengamanan barang bukti digital, hingga koordinasi lintas sektor dalam menangani kasus credential stealing. Ketentuan UU ITE belum menyediakan aturan teknis operasional sehingga aparat kerap menghadapi ambiguitas prosedural, terutama dalam pengamanan perangkat elektronik yang terinfeksi malware. Pembentukan pedoman teknis ini dapat dilakukan melalui peraturan turunan atau kebijakan sektoral yang diterbitkan oleh Kementerian Komunikasi dan Informatika bekerja sama dengan kepolisian dan lembaga perbankan, sehingga penegakan hukum terhadap pelaku dapat dilakukan secara lebih terarah, terukur, dan konsisten di seluruh wilayah Indonesia(Kiki and Rakhmat 2025).
Dari perspektif industri perbankan, upaya pencegahan harus dimulai dari penguatan standar keamanan sistem elektronik yang menghubungkan bank dengan lembaga lain seperti perusahaan sekuritas dan penyedia API.
Kasus pembobolan RDN PT Panca Global Sekuritas menunjukkan bahwa celah autentikasi tanpa One-Time Password (OTP) atau Two-Factor Authentication (TFA) menimbulkan risiko tinggi terhadap integritas transaksi(Fikaz 2025). Oleh karena itu, bank dan mitra wajib menerapkan autentikasi berlapis dan audit keamanan berkala untuk memastikan API memenuhi standar keamanan yang ditetapkan oleh otoritas pengawas. Kewajiban tersebut sejalan dengan prinsip "penyelenggaraan sistem elektronik yang aman dan andal" sebagaimana diamanatkan dalam UU ITE meskipun tidak tercantum dalam pasal tertentu. Selain itu, pemantauan transaksi secara real-time perlu diperkuat agar aktivitas abnormal seperti transfer berulang dalam waktu singkat, perubahan perangkat login, atau aktivitas dari lokasi mencurigakan dapat terdeteksi sejak dini. Bank harus mengintegrasikan fraud detection engine berbasis kecerdasan buatan untuk menganalisis pola transaksi nasabah secara dinamis(Iskandar et al. 2025). Ketika anomali terdeteksi, sistem harus mampu melakukan auto-lock terhadap akun yang berisiko tanpa menunggu laporan nasabah. Langkah-langkah tersebut merupakan implementasi preventif yang dapat mengurangi ruang gerak pelaku pencurian kredensial, terutama ketika mereka memanfaatkan kredensial yang telah dicuri melalui phishing atau malware(Ghofirin 2025).
Selain penegak hukum dan institusi keuangan, strategi pencegahan juga harus menyasar pengguna sebagai elemen paling rentan dalam ekosistem mobile banking. Edukasi literasi digital harus dilakukan secara sistematis untuk mencegah pengguna mengakses tautan mencurigakan, mengunduh file APK dari luar toko aplikasi resmi, atau memberikan izin akses berbahaya kepada aplikasi tidak dikenal. Praktik sederhana seperti mengganti PIN dan kata sandi secara berkala, menghindari penggunaan jaringan publik, serta mengaktifkan fitur keamanan perangkat dapat secara signifikan mengurangi risiko pencurian kredensial. Upaya edukasi publik ini sejalan dengan tujuan perlindungan data pribadi dan keamanan transaksi sebagaimana menjadi semangat utama pengaturan dalam UU ITE. Pada tingkat regulasi, pembaruan peraturan perundang-undangan perlu dilakukan untuk mengakomodasi perkembangan modus kejahatan kredensial yang semakin kompleks. UU ITE dalam bentuknya saat ini masih menempatkan pencurian data dalam kerangka umum akses ilegal dan perolehan data tanpa hak sebagaimana Pasal 30 dan Pasal 32, belum mengatur secara khusus tindak pidana berbasis credential theft maupun penggunaan malware otomatis sebagai instrumen kejahatan. Oleh karena itu, revisi UU ITE atau penerbitan regulasi tambahan diperlukan agar rumusan delik lebih responsif terhadap serangan berbasis teknologi generasi terbaru dan sesuai dengan standar keamanan digital internasional.
Selain pembaruan UU ITE, penguatan kebijakan sektor perbankan menjadi kebutuhan mendesak. Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) perlu menerbitkan pedoman teknis yang lebih ketat mengenai standar keamanan API, kewajiban audit independen, pengamanan transaksi digital, serta mekanisme pelaporan insiden siber. Sinergi antara OJK, BI, perbankan, serta aparat penegak hukum akan menciptakan ekosistem pengamanan berlapis yang mampu mengurangi kemungkinan serangan pencurian kredensial dan mempercepat respons ketika insiden terjadi. Kerja sama lintas lembaga ini juga berfungsi untuk memastikan bahwa tindakan pencegahan tidak hanya dilakukan pada tataran normatif, tetapi benar-benar terimplementasi dalam praktik operasional industri perbankan. Dengan demikian, strategi hukum pidana dalam menghadapi pencurian kredensial memerlukan pendekatan terpadu yang melibatkan

dimensi regulatif, teknis, institusional, dan edukatif. Tanpa sinergi antar pemangku kepentingan dan pembaruan kebijakan yang sesuai dengan perkembangan teknologi, upaya penanggulangan kejahatan siber akan terus tertinggal dari adaptasi pelaku. Pendekatan multidimensional inilah yang menjadi fondasi penting dalam menciptakan keamanan mobile banking yang lebih kuat, adaptif, dan responsif terhadap ancaman cybercrime yang terus berkembang.

## KESIMPULAN

1. Modus operandi pencurian kredensial 2025 beralih ke rekayasa sosial, phishing, malware seperti Zanubis 2025, dan eksploitasi API tanpa OTP/TFA, sehingga pelaku dapat mengambil alih akun mobile banking tanpa meretas sistem inti.
2. Efektivitas sanksi pidana berdasarkan Pasal 30 jo. 46 dan Pasal 32 jo. 48 UU ITE serta Pasal 362 dan 378 KUHP masih rendah karena kendala pembuktian digital, keterbatasan forensik, lemahnya keamanan pihak ketiga, dan belum adanya pedoman khusus penanganan credential stealing.
3. Pertanggungjawaban pidana pelaku meliputi akses ilegal, perolehan data tanpa hak, pencurian/penipuan, serta pembuatan atau penyebaran malware. Asas ekstrateritorial Pasal 2 UU ITE tetap memungkinkan pemidanaan pelaku luar negeri; pertanggungjawaban korporasi juga dapat diberlakukan jika terjadi kelalaian keamanan.
4. Upaya pencegahan meliputi peningkatan kapasitas digital forensik, pembaruan SOP, penguatan keamanan API dan OTP/TFA, audit berkala, pemantauan transaksi, serta pembaruan kebijakan keamanan siber perbankan yang didukung sinergi OJK, BI, aparat penegak hukum, dan peningkatan literasi digital masyarakat.

## PUSTAKA

Bahri, Idik Saeful. 2023. *Cyber Crime Dalam Sorotan Hukum Pidana (Edisi 2023)*. Bahasa Rakyat.

Budiyanto, S H, and others. 2025. *Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia*. Sada Kurnia Pustaka.

Farahdiva, Aiva Tyanka, Siti Linda Mulyana, and Tika Permata Asri. 2025. "Implementasi Cyber Security Pada Sistem Transaksi Keuangan Digital." *JURNAL ILMIAH EKONOMI, MANAJEMEN, BISNIS DAN AKUNTANSI* 2(4): 276–89.

Fikaz, Luthfi. 2025. *Celah Keamanan API Jadi Sorotan Pembobolan RDN, Sekuritas Didesak Berbenah*.

Ghofirin, Mohammad. 2025. *Belajar Dari Kasus BSI, Begini Cara Aman Gunakan Layanan Perbankan*.

Indradjaja, Manayra Aisha Putri, Sigid Suseno, and Budi Arta Atmaja. 2024. "Implementasi Penyidikan Terhadap Tindak Pidana Siber Dalam Perspektif Perbandingan Hukum: Indonesia Dan Inggris Raya." *Jurnal Ilmiah Penegakan Hukum* 11(2): 162–72.

Iskandar, Rizkiani, Rika Febby Rhamadhani, Ayu Putri Utami, Syarifah Aliyah Fitrisam, and Muhammad Akbar. 2025. "Peran Kecerdasan Buatan Dalam Meningkatkan Efisiensi Dan Transparansi Pasar Keuangan: The Role of Artificial Intelligence in Improving Financial Market Efficiency and Transparency." *Economic and Education Journal (Ecoducation)* 7(1): 186–207.

Kiki, Kristanto, and Baihaki Rakhmat. 2025. "Buku Referensi Tindak Pidana Siber Di Indonesia Regulasi, Tantangan, Dan Penegakan Hukum."

Mukhra, Uly Handayani, Jasman J Makruf, T Meldi Kesuma, Ahmad Nizam, and M Ridha Siregar. 2024. *Mobile Banking Dalam Persepsi Privasi Nasabah*. Syiah Kuala University Press.

Mulianingsih, Ferani, Fajar Fajar, and Suharyati Suharyati. 2025. "Manajemen Risiko Digital: Strategi Keamanan Siber Untuk Mitigasi Ancaman Di Era Revolusi Industri 4.0." *Indonesian Research Journal on Education* 5(2): 888–98.

Nainggolan, Andri Ebenezer. 2025. "Kajian Kritis Efektivitas Sanksi Pidana Dalam Kejahatan Siber Menurut Hukum Positif." *HARISA: Jurnal Hukum, Syariah, dan Sosial* 2(1)): 67–80.

Pakpahan, Bani David Soaloon, Parameshwara Parameshwara, Kartina Pakpahan, Margaretha Citra Novriyanti Saota, and Franciscus Orlando Tambunan. 2023. "Tinjauan Yuridis Kejahatan Di Dalam Sistem Elektronik Pada Rekening Virtual." *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam* 5(2): 1691–1708.

Putra, Tomi Wicaksono, Hamidah Abdurrachman, and Achmad Irwan Hamzani. 2023. *Pertanggungjawaban Pidana Terhadap Kejahatan Hacking*. Penerbit NEM.

Redaksi, CNBC Indonesia. 2025. *Awas Malware Baru Di HP Android Bobol M-Banking, Rekening Ludes!*

Rianda, Faizah Uhti. 2025. "Urgensi Pengaturan Central Bank Digital Currency Untuk Melindungi Data Pribadi Dari Cybercrime Di Indonesia." Universitas Islam Negeri Maulana Malik Ibrahim.

Rinaldi, Farrel Ardan, and Bintang Kusuma Wijaya. 2025. "Efektivitas Penegakan Hukum Terhadap Tindak Pidana Perbankan: Studi Kasus Pembobolan Dana Nasabah." *PENG: Jurnal Ekonomi Dan Manajemen* 2(3): 3437–47.

Risko, Miftahul, and Handaru Lumintang Bagus Krisnadi. 2025. "Penegakan Hukum Pidana Dan Penanggulangan Perkara Tindak Pidana Penipuan Melalui Transfer Mobile Banking." *Jurnal Terekam Jejak* 3(1): 1–12.

Rizqullah, Mhd Raihan, Rahmat Surkhalid Nasution, Sabda Abdillah Lubis, Muhammad Ichsan Parinduri, and Limrogate Immanuel. 2025. "Tindak Pidana Penyebaran Aplikasi Malware Berbasis APK: Studi Terhadap Fenomena Modus Lowongan Kerja Dan Paket Palsu." *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora* 4(3): 858–67.

Sadzili, Iza, and Lastuti Abubakar. 2025. "Doktrin Kelalaian Kontribusi (Contributory Negligence) Terhadap Tanggung Jawab Bank Atas Kerugian Nasabah Akibat Kesalahan Atau Kelalaian Pegawai Bank." *Jurnal Ilmiah Penegakan Hukum* 12(1): 1–11.

Santoso, Joseph Teguh. 2023. "Teknologi Keamanan Siber (Cyber Security)." *Penerbit Yayasan Prima Agus Teknik*: 1–173.

Saputri, Adhalia Septia, and Lusia Sulastri. 2025. "Penerapan Asas Ultimum Remedium Dalam Pemidanaan Tindak Pidana Pencucian Uang." *Journal of Mandalika Literature* 6(1): 244–50.

Wibowo, Arief, Yehu Wangsajaya, and Asep Surahmat. 2023. *Pemolisian Digital Dengan Artificial Intelligence*. PT. RajaGrafindo Persada-Rajawali Pers.