Jurnal Kompilasi Hukum
Volume 10, No. 2, December 2025, E-ISSN 2598-6414, P-ISSN 2502-5333
Publisher Magister of Law, Faculty of Law Mataram University,
open access at : http://jkh.unram.ac.id

TINDAK PIDANA PEMBOBOLAN REKENING SEBAGAI *PREDICATE CRIME* DALAM PENCUCIAN UANG: ANALISIS NORMATIF TERHADAP EFEKTIVITAS PENEGAKAN HUKUM DI INDONESIA

Elshirah Triani Cory
Fakultas Hukum Universitas Bengkulu
elshirahcory@gmail.com

Vina Putri Afisako
Fakultas Hukum Universitas Bengkulu
vinaputri148@gmail.com

Ade Risva Sari
Fakultas Hukum Universitas Bengkulu
aderisvasarii@gmail.com

Mardhatillah
Fakultas Hukum Universitas Bengkulu
mmardhatillah@unib.ac.id

ABSTRAK

Tindak pidana pembobolan rekening merupakan bentuk kejahatan ekonomi berbasis teknologi yang semakin berkembang dan berpotensi kuat menjadi tindak pidana asal *(predicate crime)* dalam pencucian uang. Penelitian ini bertujuan menganalisis pengaturan hukum positif serta efektivitas penegakan hukum terhadap pembobolan rekening khususnya rekening *dormant* (rekening tidur) dalam kaitannya dengan rezim tindak pidana pencucian uang di Indonesia. Dengan menggunakan metode penelitian hukum normatif melalui pendekatan perundang-undangan, konseptual, dan kasus, tulisan ini menelaah ketentuan dalam UU TPPU, UU ITE, UU PPSK, serta regulasi sektor perbankan yang terkait. Hasil penelitian menunjukkan bahwa meskipun secara normatif pembobolan rekening memenuhi kualifikasi sebagai *predicate crime*, efektivitas penegakan hukum masih terhambat oleh lemahnya deteksi siber perbankan, tidak adanya sistem peringatan dini antarbank, keterbatasan forensik digital aparat penegak hukum, serta fragmentasi koordinasi antara Polri, PPATK, OJK, dan lembaga keuangan. Studi kasus pembobolan rekening dormant senilai Rp.204.000.000.000,- (Dua Ratus Empat Miliar Rupiah) memperlihatkan bahwa kejahatan ini dilakukan secara terstruktur oleh sindikat yang

 DOI: https://doi.org/10.29303/jkh.v10i2.268

memadukan kejahatan *siber, insider threat,* dan pencucian uang, sehingga menuntut pembaruan regulasi dan integrasi sistem pelacakan dana secara *real time.* Hasilnya perlu penguatan harmonisasi regulasi, peningkatan kapasitas forensik digital, serta optimalisasi kedudukan LHA PPATK sebagai alat bukti untuk meningkatkan efektivitas penegakan hukum terhadap kejahatan perbankan yang berorientasi pada penyamaran hasil kejahatan.
Kata kunci: Pembobolan Rekening, Tindak Pidana Pencucian Uang, *Predicate Crime*, Kejahatan Siber, Penegakan Hukum.

ABSTRACT

Account hacking is a growing form of technology-based economic crime with strong potential to become a predicate crime in money laundering. This study aims to analyze positive legal regulations and the effectiveness of law enforcement against account hacking, particularly dormant accounts, in relation to the money laundering criminal regime in Indonesia. Using normative legal research methods through statutory, conceptual, and case-based approaches, this paper examines the provisions of the Money Laundering Law (AML/TPPU), the Electronic Information and Transactions Law (ITE), the Financial Conduct and Substances Protection Law (PPSK), and related banking sector regulations. The results indicate that although account hacking qualifies as a predicate crime, effective law enforcement is still hampered by weak banking cyber detection, the absence of an interbank early warning system, limited digital forensics capabilities of law enforcement officers, and fragmented coordination between the Indonesian National Police (Polri), the Financial Transaction Reports and Analysis Center (PPATK), the Financial Services Authority (OJK), and financial institutions. A case study of the breach of a dormant account worth Rp204,000,000,000 (Two Hundred and Four Billion Rupiah) demonstrates that this crime was perpetrated in a structured manner by a syndicate combining cybercrime, insider threats, and money laundering. This necessitates regulatory reform and the integration of a real-time fund tracking system. The findings call for strengthened regulatory harmonization, increased digital forensics capacity, and optimization of the PPATK's LHA (Account Reporting and Analysis Center) as evidence to enhance the effectiveness of law enforcement against banking crimes focused on disguising the proceeds of crime.

Keywords: *Account Hacking, Money Laundering, Predicate Crime, Cybercrime, Law Enforcement.*

PENDAHULUAN

Keberadaan lembaga perbankan di Indonesia memiliki peranan penting dalam mendukung pelaksanaan pembangunan nasional yang bertujuan mewujudkan kesejahteraan masyarakat. Melalui aktivitasnya, bank diharapkan mampu mempercepat pemerataan hasil pembangunan, mendorong pertumbuhan ekonomi, serta menjaga stabilitas nasional agar arah pembangunan menuju peningkatan taraf hidup rakyat dapat tercapai.[1] Dengan menjalankan fungsi utama sebagai penghimpun dana dari masyarakat dan penyalur kembali dana tersebut ke sektor produktif,[2] bank memiliki peran strategis dalam menggerakkan partisipasi masyarakat terhadap peningkatan perekonomian nasional secara menyeluruh, sekaligus membantu memperkuat kondisi ekonomi masyarakat di tingkat individu maupun kelompok kecil.

Perkembangan teknologi informasi dan komunikasi di era digital telah membawa dampak besar terhadap sistem keuangan dan perbankan di Indonesia. Transformasi digital mempermudah masyarakat dalam melakukan transaksi keuangan secara cepat, efisien, dan lintas platform. Namun, di sisi lain, kemajuan ini juga menciptakan celah baru bagi munculnya bentuk-bentuk kejahatan ekonomi berbasis teknologi. Salah satu fenomena yang menonjol adalah tindak pidana pembobolan rekening, di mana pelaku memanfaatkan sistem elektronik untuk memperoleh keuntungan secara melawan hukum.[3] Kejahatan ini tidak hanya berdampak pada stabilitas sistem perbankan, tetapi juga berpotensi menjadi *predicate crime* dalam praktik pencucian uang (*money laundering*). Oleh karena itu, muncul kebutuhan mendesak akan perlindungan hukum yang adaptif dan efektif dalam menghadapi kejahatan ekonomi modern di era digital.

Fenomena aktual menunjukkan peningkatan kasus pembobolan rekening dengan modus operandi yang semakin canggih dan terorganisir. Salah satu kasus menonjol adalah pembobolan rekening dormant senilai Rp.204.000.000.000,- (Dua Ratus Empat Miliar Rupiah) pada bank milik negara yang terungkap pada September 2025.[4] Kasus ini memperlihatkan kompleksitas kejahatan di mana pelaku memanfaatkan akses ilegal ke

---

[1] Malayu S. P. Hasibuan, Dasar-Dasar Perbankan, PT. Bumi Aksara, Jakarta, 2001, hlm. 4.

[2] *Ibid*

[3] Khudsiyah, D., Rahmadan, D., & Erdianto, E. (2025). Penegakan Hukum Terhadap Modus Baru Kejahatan Cyber Berupa Rekayasa Informasi Teknologi Pembobolan Rekening Nasabah Melalui Internet Banking. *Jurnal Ilmiah Wahana Pendidikan*, *11*(8.D), hlm. 237.

[4] Pusat Pelaporan dan Analisis Transaksi Keuangan. 2025. Bareskrim Polri Ungkap Kasus Pembobolan Rekening Dorman Bank BUMN Rp204 Miliar, Terkait Kejahatan Siber dan Pencucian Uang. Diakses pada 30 Oktober 2025 dari https://www.ppatk.go.id/news/read/1529/bareskrim-polri-ungkap-kasus-pembobolan-rekening-dorman-bank-bumn-rp204-miliar-terkait-kejahatan-siber-dan-pencucian-uang.html

sistem perbankan di luar jam operasional untuk melakukan transfer cepat ke berbagai rekening dan dompet digital. Selain itu, ditemukan pula keterlibatan berlapis antara oknum internal bank, pelaku eksternal, serta pihak ketiga yang berperan sebagai *nominee* dan pelaku pencucian uang. Kasus ini menunjukkan bahwa pembobolan rekening bukan sekadar kejahatan siber, melainkan juga kejahatan ekonomi terorganisir yang dapat berfungsi sebagai *predicate crime* dalam tindak pidana pencucian uang.

Secara normatif, tindak pidana ini diatur dan dikaitkan dengan beberapa regulasi, antara lain Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan UU No. 19 Tahun 2016 (UU ITE), Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana, Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU PPSK), serta ketentuan umum dalam Kitab Undang-Undang Hukum Pidana (KUHP) Pasal 55 tentang penyertaan. Kompleksitas muncul karena kejahatan ini melibatkan berbagai rezim hukum sekaligus yaitu hukum pidana umum, hukum siber, hukum perbankan, dan hukum keuangan. Tantangan utama terletak pada aspek pembuktian digital, pelacakan aliran dana lintas platform, serta koordinasi antar lembaga penegak hukum seperti Polri, PPATK, OJK, dan Kejaksaan. Kondisi tersebut memperlihatkan adanya kesenjangan antara norma hukum positif dengan kebutuhan penegakan hukum yang responsif terhadap dinamika kejahatan ekonomi digital.

Permasalahan normatif yang timbul adalah apakah kerangka hukum yang ada sudah memadai untuk mengkualifikasikan pembobolan rekening sebagai *predicate crime* dalam tindak pidana pencucian uang. Selain itu, muncul persoalan mengenai penerapan pertanggungjawaban pidana terhadap pelaku yang memiliki peran berbeda, baik internal maupun eksternal, serta terhadap pihak-pihak yang terlibat secara tidak langsung melalui mekanisme *layering* atau *placement*. Di sisi teoretis, juga terdapat perdebatan mengenai konsep *concursus* dan delik berlapis dalam konteks kejahatan digital yang bersifat lintas sistem dan lintas yurisdiksi. Oleh karena itu, diperlukan pendekatan konseptual baru untuk menafsirkan pertanggungjawaban pidana kolektif dalam tindak pidana ekonomi digital.

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada analisis normatif terhadap pengaturan hukum dan efektivitas penegakan hukum terhadap tindak pidana pembobolan rekening sebagai *predicate crime* dalam tindak pidana pencucian uang di Indonesia. Penelitian ini memiliki signifikansi dalam menjawab tantangan hukum pidana nasional dalam menghadapi perkembangan kejahatan ekonomi berbasis teknologi.

METODE PENELITIAN

Metode penelitian yang digunakan dalam artikel ini merupakan penelitian hukum normatif dengan sifat deskriptif-analitis. Penelitian ini berfokus pada pengkajian norma-norma hukum positif, asas hukum, dan doktrin yang relevan terhadap penerapan hukum pidana dalam kasus pembobolan rekening dormant sebagai *predicate crime* tindak pidana pencucian uang. Tujuan dari penelitian ini adalah memberikan gambaran menyeluruh serta analisis mendalam mengenai penerapan norma hukum pidana ekonomi dan tindak pidana siber dalam konteks sistem keuangan Indonesia.

Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) untuk menelaah ketentuan dalam UU No. 8 Tahun 2010, UU ITE, UU No. 4 Tahun 2023, KUHP, serta peraturan PPATK dan Bank Indonesia; pendekatan konseptual (c*onceptual approach*) untuk memahami konsep *predicate crime*, *mens rea*, *actus reus*, dan pertanggungjawaban pidana korporasi; serta pendekatan kasus (*case approach)* terhadap perkara pembobolan rekening dormant senilai Rp.204.000.000.000,- (Dua Ratus Empat Miliar Rupiah). Data penelitian diperoleh melalui studi kepustakaan terhadap bahan hukum primer, sekunder, dan tersier. Seluruh bahan hukum dianalisis secara kualitatif normatif dengan menafsirkan ketentuan hukum yang berlaku dan mengaitkannya dengan asas hukum pidana, sehingga menghasilkan argumentasi hukum yang logis, sistematis, dan dapat dipertanggungjawabkan secara akademik.

HASIL DAN PEMBAHASAN

A. Pengaturan Hukum Positif di Indonesia terhadap Tindak Pidana Pembobolan Rekening dan Kaitannya dengan Tindak Pidana Pencucian Uang sebagai Kejahatan Asal (*Predicate Crime*)

Pembobolan rekening merupakan salah satu manifestasi kejahatan perbankan dan siber yang secara nyata menghantam sistem keuangan dan kepercayaan publik terhadap lembaga keuangan. Modusnya bisa berupa pencurian data nasabah, pemalsuan identitas, *phishing* atau *social engineering* untuk memperoleh kode OTP, ataupun akses tidak sah (*unauthorized access*) ke rekening, yang kemudian digunakan untuk pemindahan dana atau pengosongan saldo. Sebagai contoh nyata, Bareskrim Polri berhasil mengungkap kasus pembobolan rekening dormant di sebuah bank BUMN senilai Rp.204.000.000.000,- (Dua Ratus Empat Miliar Rupiah) yang terkait praktik kejahatan siber dan pencucian uang.[5] Dari

[5] Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), "Bareskrim Polri Ungkap Kasus Pembobolan Rekening Dorman Bank BUMN Rp204 Miliar Terkait Kejahatan Siber dan Pencucian Uang," *ppatk.go.id*, 23 Februari 2024, diakses 10 November 2025,

perspektif hukum perbankan, pembobolan rekening dikategorikan sebagai kejahatan kerah putih (*white collar crime*) yang menggunakan kecanggihan teknologi dan pemahaman sistem keuangan secara mendalam. Kejahatan ini tidak hanya melibatkan tindakan melawan hukum dalam pengelolaan data dan dana nasabah, tetapi juga mencerminkan lemahnya pengawasan internal bank serta sistem keamanan perbankan dalam melindungi hak nasabah.[6] Hal ini menuntut pengaturan hukum yang mengakomodasi sifat hybrid antara kejahatan teknologi dan kejahatan ekonomi.

Berkaitan dengan kejahatan pencucian uang, undang-undang Indonesia mengakui bahwa tindak pidana asal (*predicate crime*) menjadi sumber harta kekayaan yang akhirnya dilapisi dan disamarkan melalui mekanisme pencucian uang. Menurut Pasal 2 Ayat (1) Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU), menyebut "Harta Kekayaan yang diperoleh dari tindak pidana … merupakan hasil tindak pidana pencucian uang." Dengan demikian, setiap dana yang diperoleh melalui pembobolan rekening bila dilakukan secara melawan hukum dan memenuhi unsur-unsur delik dapat dikualifikasikan sebagai kejahatan asal yang membuka jalan bagi penegakan aturan pencucian uang.

Penegakan terhadap pembobolan rekening sebagai kejahatan asal memerlukan sinkronisasi regulasi lintas bidang yang mencakup aspek hukum siber, perbankan, dan anti-pencucian uang. Di satu sisi, tindak pidana siber seperti akses tanpa hak dan transfer dana ilegal termasuk dalam ruang lingkup kejahatan teknologi informasi yang diatur oleh regulasi siber. Di sisi lain, peredaran dana hasil kejahatan melalui sistem keuangan formal secara otomatis melibatkan mekanisme pengawasan dan pelaporan transaksi mencurigakan yang berada di bawah otoritas lembaga keuangan. Dalam praktiknya, tantangan utama muncul karena belum adanya integrasi menyeluruh antar sistem pelaporan dan pengawasan, sehingga koordinasi antara lembaga pengawas seperti Bank Indonesia, OJK, dan PPATK belum sepenuhnya efektif. tanpa adanya keselarasan sistem regulasi dan pelaporan transaksi digital antar lembaga, upaya deteksi serta penindakan terhadap

https://www.ppatk.go.id/news/read/1529/bareskrim-polri-ungkap-kasus-pembobolan-rekening-dorman-bank-bumn-rp204-miliar-terkait-kejahatan-siber-dan-pencucian-uang.html.

[6] Almira Qurrotul Aini and Elanti Fatayatun Khoiroh, "Perlindungan Hukum Nasabah Dalam Kasus Pembobolan Rekening Bank Di Indonesia," *Jurnal Multidisiplin Ilmu Akademik* 1, no. 6 (2024): 168.

kejahatan keuangan digital rawan menghadapi celah hukum yang dapat dimanfaatkan pelaku kejahatan.[7]

Regulasi terkait kejahatan siber seperti Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahan melalui Undang-Undang Nomor 19 Tahun 2016 perlu dilihat dalam konteks ini karena pembobolan rekening sering melibatkan elemen akses atau manipulasi data elektronik. Regulasi keuangan seperti Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU PPSK) juga mengatur penguatan integritas sistem keuangan. Namun, meskipun regulasi-regulasi tersebut ada, belum terdapat pedoman teknis yang secara spesifik mengatur pembobolan rekening sebagai *predicate crime* dan tahapan pelacakan dana hasil kejahatan tersebut hingga ke rekening bank dan sistem keuangan formal.

Dalam konteks pengawasan dan pencegahan tindak pidana pembobolan rekening, tantangan utama yang dihadapi sistem hukum Indonesia terletak pada belum optimalnya sinergi dan harmonisasi regulasi antara otoritas keuangan dan lembaga pengawas sektor perbankan. Walaupun Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK) telah berupaya memperkuat koordinasi melalui *Forum Koordinasi Makroprudensial Mikroprudensial (FKMM)* serta menerbitkan regulasi terkait ketahanan dan keamanan siber, implementasi di lapangan masih menunjukkan berbagai kendala.[8] Salah satunya adalah ketidakterpaduan sistem pengawasan dan pelaporan antar lembaga keuangan, sehingga aliran dana hasil kejahatan digital, termasuk hasil pembobolan rekening, sering kali sulit dilacak secara real time. Kurangnya integrasi data dan standar keamanan digital yang seragam juga memperbesar risiko kebocoran data serta memperlambat proses identifikasi aset hasil kejahatan yang berpotensi menjadi *predicate crime* dalam tindak pidana pencucian uang.

Selain itu, terdapat kekosongan hukum terkait penanganan alur dana hasil pembobolan rekening. Undang-undang pencucian uang menyebut bahwa harta kekayaan dari tindak pidana (termasuk yang di bidang perbankan) merupakan objek pencucian uang, namun tidak menyebut secara eksplisit "pembobolan rekening" sebagai kejahatan asal.

[7] Firzatul Rima Fitriana and Nuryanto A Daim, "Peran PPATK Dalam Mengungkap Tindak Pidana Pencucian Uang Hasil Dari Tindak Pidana Korupsi," *Law and Humanity* 3, no. 1 (2025): 21-22.

[8] Meyrara Widya Putri and Jefry Tarantang, "Optimalisasi Regulasi Perbankan Untuk Mempercepat Transformasi Digital Di Indonesia," *Belom Bahadat: Jurnal Hukum Agama Hindu* 15, no. 1 (2025): 19-22.

Dalam praktiknya ini berarti bahwa dana yang diperoleh melalui pembobolan rekening terkadang sulit dikategorikan sebagai hasil tindak pidana dalam penanganan TPPU. Hal ini menimbulkan kesenjangan antara norma hukum dan praktik lapangan, yang pada akhirnya melemahkan mekanisme pencegahan dan penindakan pencucian uang.

Dalam aspek implementasi, peraturan pelaksana dari PPATK, OJK dan BI menentukan bagaimana mekanisme pelaporan transaksi mencurigakan, pembekuan rekening, dan kerjasama internasional dalam pemblokiran dana. Namun, regulasi tersebut sering bersifat umum dan belum spesifik terhadap pembobolan rekening digital dan siber. Ini memunculkan risiko bahwa pelaku pembobolan rekening bisa "menyembunyikan" dana melalui multi-rekening, transfer lintas negara, atau penggunaan kripto tanpa terdeteksi. Oleh karena itu, perlu ada kebijakan yang memperkuat kewajiban pelaporan, unit forensik bank, dan mekanisme pelacakan dana hasil pembobolan sebagai bagian dari rangkaian predicate crime.

Secara keseluruhan, pengaturan hukum positif Indonesia sudah menyediakan kerangka dasar yang memungkinkan pelaksanaan penegakan terhadap kejahatan pembobolan rekening dan pencucian uang, namun efektivitasnya masih terbatas oleh hambatan normatif, teknis, dan institusional. Untuk memperkuat upaya penegakan tersebut, diperlukan pembaruan regulasi yang secara eksplisit menghubungkan pembobolan rekening dengan pencucian uang, memperkuat pedoman teknik pelacakan dana (*follow the money*), serta memastikan harmonisasi antar-regulasi perbankan, siber, dan keuangan. Dengan demikian, upaya pencegahan dan penegakan hukum akan menjadi lebih sistemik dan komprehensif dalam menghadapi kejahatan ekonomi berbasis digital.

B. Efektivitas Penegakan Hukum Terhadap Kejahatan Pembobolan Rekening yang Terintegrasi dengan Pencucian Uang dalam Praktik Penegakan Hukum di Indonesia

Efektivitas penegakan hukum terhadap tindak pidana pembobolan rekening yang berkelindan dengan tindak pidana pencucian uang tidak hanya ditentukan oleh keberadaan norma hukum positif, tetapi juga oleh sejauh mana norma tersebut dapat diterapkan secara konsisten, terukur, dan adaptif terhadap perkembangan modus kejahatan digital. Penegakan hukum atas kejahatan ini bersifat multidimensional karena melibatkan aspek kejahatan perbankan, siber, dan anti-pencucian uang, sehingga membutuhkan tata kelola kelembagaan dan kapasitas penegakan yang terintegrasi. Dalam konteks Indonesia, efektivitas tersebut masih menghadapi sejumlah hambatan yang bersifat struktural, teknis, maupun konseptual.

Kapasitas deteksi, pencegahan, dan pengawasan perbankan Indonesia terhadap serangan siber masih belum mencapai tingkat yang memadai untuk menghadapi kompleksitas ancaman digital saat ini. Meskipun Otoritas Jasa Keuangan (OJK) dan Bank Indonesia telah menerbitkan berbagai regulasi tentang keamanan dan ketahanan sistem teknologi informasi termasuk *Panduan Resiliensi Digital* OJK tahun 2024 implementasi di tingkat industri menunjukkan variasi yang sangat lebar. Sejumlah bank masih menempatkan keamanan siber sebatas kepatuhan administratif, bukan strategi mitigasi risiko yang bersifat struktural di mana manajemen risiko siber di sektor jasa keuangan belum diimplementasikan secara keseluruhan, khususnya dalam aspek kesiapan teknologi, tata kelola, dan respons insiden.[9] Di sisi lain, ketergantungan bank pada sistem deteksi berbasis *rule-based monitoring* yang hanya mengandalkan *threshold* sederhana membuat serangan dengan pola *low signature* atau anomali perilaku dapat lolos dari pantauan, ini menunjukkan lemahnya penggunaan sistem keamanan berlapis serta kemampuan adaptif perbankan dalam menghadapi ancaman malware dan *social engineering*.[10]

Kelemahan ini semakin diperburuk oleh absennya *real-time interbank alert system* yang memungkinkan koordinasi cepat antar lembaga perbankan. Padahal, dalam praktik pembekuan dana hasil kejahatan siber (*rapid freezing*), rentang waktu lima hingga sepuluh menit pertama merupakan fase paling menentukan untuk mencegah perpindahan dana ke rekening penampung. Sayangnya, tidak adanya sistem peringatan lintas bank menyebabkan proses notifikasi dan verifikasi antarbank berjalan lambat, sehingga *window of opportunity* bagi pelaku kejahatan tetap terbuka. Kesiapan infrastruktur *cyber security* dan forensik digital antarbank di Indonesia masih tidak merata; sebagian bank memiliki perangkat analisis log yang baik, namun sebagian lain belum mampu melakukan investigasi digital secara cepat ketika insiden terjadi.[11] Keterbatasan kapabilitas forensik ini juga diperkuat oleh kurangnya tenaga ahli TI perbankan yang memiliki spesialisasi dalam *incident response*, analisis log, atau identifikasi pola pencucian uang berbasis transaksi digital.

Dari sisi ancaman, pencurian data nasabah dan kejahatan berbasis rekayasa sosial terus meningkat. Adanya kelemahan pada pengamanan data internal bank dan rendahnya literasi keamanan digital nasabah membuat perbankan semakin rentan terhadap serangan

[9] Luthfah, D. (2024). Penguatan Keamanan Siber Pada Sektor Jasa Keuangan Indonesia. *Jurnal Penelitian Dan Karya Ilmiah Lembaga Penelitian Universitas Trisakti*, *9*, hal. 264

[10] Afifah, E. F. N., Simatangkir, D. W. E., & Faliha, N. S. (2025). Keamanan Siber Dalam Perbankan Serta Tantangan Dan Solusi Di Era Digital. *Jurnal Multidisiplin Ilmu Akademik*, *2*(1), hal. 38

[11] Dermawan, I., Baidawi, A., & Dewi, S. M. (2023). Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia. *Jurnal Informasi Dan Teknologi*, *5*(3), hal. 23

yang menargetkan informasi pribadi dan kredensial akses.[12] Akibatnya, sejumlah insiden pembobolan rekening *dormant* (rekening tidur) maupun rekening aktif dapat terjadi tanpa memberikan sinyal risiko awal bagi sistem teknologi bank. Selain itu, regulasi terkait pelaporan insiden siber kepada OJK atau lembaga lain seperti PPATK masih berjalan secara terpisah dan tidak bersifat *real-time*, sehingga potensi aktivasi *early warning system* belum dapat dimaksimalkan. Hal ini selaras berdasarkan laporan pada *Bisnis.com* tahun 2023 yang menyebutkan bahwa bank-bank Indonesia menerima ribuan serangan siber setiap hari namun tidak semuanya dapat ditangani dengan respons cepat dan terkoordinasi.[13]

Dari keseluruhan dinamika tersebut terlihat jelas bahwa kapasitas deteksi dan pencegahan perbankan Indonesia masih membutuhkan penguatan signifikan, baik dalam aspek teknis, tata kelola, maupun koordinasi antar lembaga. Modernisasi sistem deteksi berbasis *behavioural analytics*, integrasi *real-time alert system* antar lembaga, penguatan kapabilitas forensik digital, serta peningkatan koordinasi antara OJK, BI, PPATK, dan industri perbankan menjadi langkah fundamental untuk menutup celah kerentanan yang hingga kini masih dimanfaatkan pelaku kejahatan siber.

Kasus pembobolan rekening *dormant* (rekening tidur) senilai Rp.204.000.000.000,- (Dua Ratus Empat Miliar Rupiah) di sebuah bank BUMN pada September 2025 dapat dijadikan mikrokosmos untuk membedah anatomi tantangan penegakan hukum.[14] Kasus ini membuktikan bahwa kejahatan perbankan modern tidak lagi bersifat *opportunistic* (mencari peluang), melainkan telah bertransformasi menjadi *structured* (terstruktur) dan *targeted* (tertarget). Pemilihan *rekening dormant* sebagai target bukanlah kebetulan, melainkan pilihan strategis.[15] Rekening *dormant* memiliki tingkat pengawasan yang minim, baik dari pemilik rekening maupun dari sistem internal bank, sehingga memberikan waktu dan ruang yang leluasa bagi pelaku untuk beroperasi tanpa

[12] Balaka, KI, Hakim, AR, & Sulistyany, FD (2024). Pencurian Informasi Nasabah di Sektor Perbankan: Ancaman Serius di Era Digital. *Justitiabelen* , *10* (2), hal. 115

[13] Burhan, F. A. (2023, Maret 9). *Industri finansial banjir serangan siber, bank digital pasang kuda-kuda*. Bisnis.com. https://finansial.bisnis.com/read/20230309/90/1635655/industri-finansial-banjir-serangan-siber-bank-digital-pasang-kuda-kuda

[14] Pusat Pelaporan dan Analisis Transaksi Keuangan. (n.d.). *Bareskrim Polri ungkap kasus pembobolan rekening Dorman Bank (BUMN) Rp 204 miliar terkait kejahatan siber dan pencucian uang*. https://www.ppatk.go.id/news/read/1529/bareskrim-polri-ungkap-kasus-pembobolan-rekening-dorman-bank-bumn-rp204-miliar-terkait-kejahatan-siber-dan-pencucian-uang.html

[15] Humas Polri. *Bareskrim Polri ungkap sindikat pembobolan rekening dormant senilai Rp204 miliar, 9 tersangka diamankan*. https://humas.polri.go.id/news/detail/2102172-bareskrim-polri-ungkap-sindikat-pembobolan-rekening-dormant-senilai-rp204-miliar-9-tersangka-diam

memicu peringatan (*red flag*). Kejahatan ini merupakan *hybrid crime* yang menggabungkan tiga elemen sekaligus: (1) Kelemahan prosedural internal bank (status *dormant*), (2) Keterlibatan oknum internal (*insider threat*), dan (3) Kecanggihan teknologi siber (*cyber threat*).[16]

Pengungkapan oleh Bareskrim Polri menunjukkan bahwa sindikat ini terdiri dari tiga klister yang bekerja secara terintegrasi:

(1) Klaster Internal (Oknum Bank): Terdiri dari AP (Kepala Cabang Pembantu) dan GRH (*Consumer Relation Manager*). Peran mereka krusial: memberikan akses ke *core banking system* yang memungkinkan eksekutor melakukan transaksi pemindahan dana secara *in absentia* (tanpa kehadiran fisik nasabah).
(2) Klaster Eksekutor (Pelaku Pembobolan): Terdiri dari C alias K (*mastermind* yang menyamar sebagai "Satgas Perampasan Aset"), DR (konsultan hukum yang memberi justifikasi legal palsu), NAT (eks-pegawai bank yang bertindak sebagai eksekutor teknis akses ilegal dan pemindahbukuan), R (mediator yang menghubungkan sindikat dengan oknum bank), dan TT (fasilitator keuangan).
(3) Klaster Pencucian Uang: Terdiri dari DH dan IS, yang berperan menyiapkan rekening penampungan dan mengelola aliran dana hasil kejahatan untuk disamarkan.[17]

Struktur sindikat ini menunjukkan bahwa *predicate crime* (pembobolan rekening oleh Klaster 1 dan 2) dan tindak pidana pencucian uang (oleh Klaster 3) bukanlah dua tindak pidana yang terpisah dan berurutan. Keduanya direncanakan secara simultan sebagai satu operasi terintegrasi. Keberadaan “Klaster Pencucian Uang” (DH dan IS) yang telah siap dengan rekening penampungan membuktikan bahwa *tujuan akhir* (pencucian uang) sudah dirancang *sebelum predicate crime* (pembobolan) dieksekusi.[18] Hal ini menantang pendekatan penegakan hukum tradisional yang seringkali memisahkan penyidikan *predicate crime* (ditangani oleh Direktorat Reserse Kriminal Umum/Khusus) dengan penyidikan TPPU (ditangani oleh Direktorat Tindak Pidana Ekonomi dan Khusus). Kasus ini juga memperlihatkan eskalasi kejahatan, di mana para pelaku utama (*mastermind* C dan

[16] Siti Yona Hukmana. Ini *peran 9 tersangka pembobol rekening dormant bank pemerintah senilai Rp204 miliar*. MetroTV News. https://www.metrotvnews.com/read/NleC8v78-ini-peran-9-tersangka-pembobol-rekening-dormant-bank-pemerintah-senilai-rp204-miliar

[17] Puslit & BK DPR RI. (2025, September). *Isu Sepekan – IV: Pengungkapan sindikat pembobol rekening dormant* (No. 2046). https://berkas.dpr.go.id/pusaka/files/isu_sepekan/Isu%20Sepekan---IV-PUSLIT-September-2025-2046.pdf

[18] *Ibid*

pelaku TPPU DH) juga terlibat dalam penculikan dan pembunuhan seorang Kepala Cabang Bank lain (Muhammad Ilham Pradipta) yang menolak untuk diajak bekerja sama.[19] Ini mematahkan citra *white-collar crime* sebagai kejahatan "tanpa kekerasan" dan menunjukkan tingkat bahaya yang setara dengan kejahatan terorganisir konvensional.

Untuk memvisualisasikan kompleksitas ini, pemetaan peran sindikat dan jerat hukum yang digunakan disajikan dalam tabel berikut:[20]

Tabel 1

Pemetaan Peran Sindikat dan Jerat Hukum dalam

Kasus Pembobolan Rekening BUMN senilai Rp.204.000.000.000,- (Dua Ratus Empat Miliar Rupiah)

Kelompok Sindikat	**Tersangka (Inisial)**	**Peran Kunci**	**Pasal Berlapis yang Diterapkan**
Oknum Karyawan Bank	AP (Kepala Cabang Pembantu)	Memberikan akses ke *core banking system* untuk transaksi *in absentia*.	UU PPSK, UU ITE, UU Transfer Dana, UU TPPU, Jo. Pasal 55 KUHP
	GRH (*Consumer Relation Manager*)	Penghubung antara sindikat eksekutor dan oknum internal (AP).	UU PPSK, UU ITE, UU Transfer Dana, UU TPPU, Jo. Pasal 55 KUHP
Pelaku Pembobolan (Eksekutor)	C alias K (*Mastermind*)	Aktor intelektual, mengaku sebagai "Satgas Perampasan Aset".	UU PPSK, UU ITE, UU Transfer Dana, UU TPPU, Jo. Pasal 55 KUHP
	DR (Konsultan Hukum)	Memberi perlindungan hukum palsu dan merencanakan eksekusi.	UU PPSK, UU ITE, UU Transfer Dana, UU TPPU, Jo. Pasal 55 KUHP
	NAT (Eks-Pegawai Bank)	Eksekutor teknis: melakukan *access* ilegal dan pemindahbukuan.	UU PPSK, UU ITE, UU Transfer Dana, UU TPPU, Jo. Pasal 55 KUHP
	R (Mediator)	Mencari dan mengenalkan oknum bank (AP) kepada sindikat.	UU PPSK, UU ITE, UU Transfer Dana, UU TPPU, Jo. Pasal 55 KUHP
	TT (Fasilitator Keuangan)	Mengelola uang hasil kejahatan.	UU PPSK, UU ITE, UU Transfer Dana, UU TPPU, Jo. Pasal 55 KUHP

[19] *Ibid*

[20] Humas Polri, Op.Cit

Pelaku Pencucian Uang	DH	Bekerja sama membuka blokir rekening dan memindahkan dana terblokir.	UU TPPU, UU Transfer Dana, Jo. Pasal 55 KUHP
	IS	Menyiapkan rekening penampungan dan menerima aliran dana kejahatan.	UU TPPU, UU Transfer Dana, Jo. Pasal 55 KUHP

Efektivitas penegakan hukum dalam perkara kejahatan siber pada dasarnya mengalami hambatan signifikan yang bersumber dari persoalan teknis penyidikan dan pembuktian. Hambatan tersebut bersifat fundamental dan sistemik, terutama terkait dengan keterbatasan kapasitas institusional aparat penegak hukum (APH).[21] Pertama, minimnya sumber daya manusia yang memiliki kompetensi forensik digital menyebabkan proses penegakan hukum tidak mampu beradaptasi dengan kompleksitas modus operandi kejahatan siber. Dalam konteks ini, akses rekening bank selain oleh pihak bank sendiri sangat krusial bagi lembaga-lembaga penegak hukum dan pengawasan guna mendukung investigasi dan penindakan tindak pidana, termasuk kejahatan siber. Pihak-pihak yang berwenang mengakses rekening bank selain pihak bank adalah: (1) Kepolisian Republik Indonesia, yang memiliki kewenangan sebagai penyidik tindak pidana asal maupun tindak pidana pencucian uang (TPPU), (2) Pusat Pelaporan dan Analisis Transaksi Keuangan Mencurigakan (PPATK), yang bertugas sebagai lembaga intelijen keuangan untuk memantau dan menganalisis transaksi mencurigakan, (3) Otoritas Jasa Keuangan (OJK), yang berfungsi sebagai otoritas pengawas sistem perbankan dan dapat mengakses rekening untuk kepentingan pengawasan dan penyidikan, (4) Kejaksaan sebagai penuntut umum, yang memiliki hak mengakses rekening terkait proses penuntutan perkara pidana.[22] Kegiatan penyidikan yang mensyaratkan kemampuan untuk mengamankan, mengekstraksi, dan menganalisis data digital pada praktiknya masih bergantung pada unit-unit ahli tertentu, khususnya yang terpusat di tingkat Mabes Polri, sehingga menimbulkan kemacetan dalam penanganan perkara yang secara inheren sensitif terhadap waktu. Kedua, karakter bukti digital yang bersifat sangat rentan (*volatile*) menimbulkan kesulitan tersendiri bagi penyidik. Berbeda dengan bukti fisik, data digital yang tersimpan pada perangkat keras atau server dapat dengan mudah dihapus, dimanipulasi, ataupun dienkripsi

[21] Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, *5*(02), hal. 59

[22] Pelupessy, B. E. (2025). Terobosan Hukum Dalam Rahasia Bank. *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial*, *2*(7), hal. 62-63

oleh pelaku, sehingga mempersempit ruang penyidik untuk memperoleh alat bukti yang sah menurut hukum acara pidana.[23]

Ketiga, struktur alat bukti dalam Pasal 184 KUHAP menempatkan keterangan saksi sebagai alat bukti utama, namun dalam perkara siber keberadaan saksi yang melihat, mendengar, atau mengalami langsung suatu tindak pidana hampir tidak mungkin ditemukan mengingat *locus delicti* kejahatan berada di ruang maya. Kondisi ini mengakibatkan bergesernya ketergantungan pembuktian pada keterangan ahli dan bukti petunjuk berupa data digital. Kombinasi antara minimnya tenaga ahli forensik digital dan penggunaan perangkat teknologi yang usang oleh APH berimplikasi pada rendahnya efisiensi penegakan hukum. Kesenjangan tersebut menimbulkan ketidakseimbangan yang serius, di mana kecepatan pelaku dalam mengeksekusi pembobolan dan memindahkan dana sebagaimana tercermin dalam kasus penyalahgunaan dana sebesar Rp.204.000.000.000,- (Dua Ratus Empat Miliar Rupiah) yang terjadi dalam waktu sangat singkat jauh melampaui kemampuan respons birokrasi penyidikan dan proses forensik digital.[24]

Pemberantasan tindak pidana pencucian uang (TPPU), yang pada prinsipnya berorientasi pada pelacakan aliran dana (*follow the money*), merupakan rezim penegakan hukum yang secara inheren bergantung pada sinergi antar lembaga penegak hukum dan otoritas terkait.[25] Namun, praktik di lapangan menunjukkan bahwa koordinasi tersebut seringkali terhambat oleh fragmentasi kewenangan dan kecenderungan ego sektoral. Penanganan perkara pembobolan rekening yang berkorelasi dengan TPPU, misalnya, melibatkan sedikitnya empat yurisdiksi kelembagaan yakni Kepolisian Republik Indonesia (selaku penyidik tindak pidana asal dan TPPU), Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) sebagai lembaga intelijen keuangan, Otoritas Jasa Keuangan (OJK) sebagai otoritas pengawas sistem perbankan, serta Kejaksaan sebagai penuntut umum. Fragmentasi ini berdampak pada buruknya manajemen koordinasi dan kurang optimalnya pemanfaatan produk intelijen keuangan dalam proses pembuktian.

Salah satu persoalan yang paling menonjol adalah belum efektifnya penggunaan Laporan Hasil Analisis (LHA) PPATK sebagai instrumen pembuktian. Meskipun LHA memiliki signifikansi tinggi dalam memetakan aliran dana dan pola transaksi

[23] Judijanto, L., & Nugroho, B. (2025). Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrime di Indonesia. *Sanskara Hukum dan HAM*, *3*(03), hal. 122

[24] *Ibid*, hal. 123

[25] Pusat Pelaporan dan Analisis Transaksi Keuangan. (2023, July 26). *Inffast*. https://www.ppatk.go.id/news/read/1278/inffast

mencurigakan, berdasarkan Kitab Undang-Undang Hukum Acara Pidana, sebagaimana di dalam pasal 184 KUHAP yang menyebutkan bahwa alat bukti hanya terdiri dari: keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Sehingga sistem peradilan pidana Indonesia tidak mengakui dokumen tersebut sebagai alat bukti yang berdiri sendiri di persidangan. LHA hanya berfungsi sebagai bahan petunjuk bagi penyidik, sehingga menimbulkan kesenjangan pembuktian (*evidentiary gap*) yang substansial. Kondisi ini mengharuskan penyidik untuk mengolah dan menerjemahkan temuan-intelijen yang bersifat teknis dan kompleks tersebut menjadi alat bukti yang memenuhi ketentuan Pasal 184 KUHAP. Proses ini membutuhkan waktu yang panjang, memerlukan kompetensi analisis keuangan yang relatif setara dengan analis PPATK, dan rawan mengalami kegagalan apabila penyidik tidak memiliki kapasitas teknis yang memadai.

Untuk mengatasi masalah tersebut, sejumlah solusi normatif dan prosedural telah diusulkan, salah satunya adalah optimalisasi mekanisme koordinasi sebagaimana diatur dalam Pasal 64 Undang-Undang TPPU. Optimalisasi tersebut dapat diwujudkan melalui pembentukan produk hukum baru berupa *Laporan Khusus* (LK) yang disusun secara bersama antara PPATK dan penyidik. Laporan Khusus ini dirancang untuk disumpah serta diformat sedemikian rupa agar memenuhi kualifikasi alat bukti surat sebagaimana dimaksud dalam Pasal 187 KUHAP. Jika diterapkan secara konsisten, inovasi prosedural ini berpotensi mempersempit kesenjangan pembuktian, mempercepat proses penyidikan, serta meningkatkan efektivitas pembuktian TPPU di pengadilan.

Tantangan utama dalam penegakan hukum terhadap tindak pidana pencucian uang (TPPU) pada era digital terletak pada kecepatan serta tingkat anonimitas pelaku dalam memindahkan dan menyamarkan hasil kejahatan. Modus operandi para pelaku menunjukkan evolusi yang melampaui sistem perbankan konvensional dan kini memanfaatkan instrumen keuangan berlapis yang secara sistematis dirancang untuk mengaburkan jejak transaksi. Temuan PPATK dalam kasus pembobolan dana sebesar melibatkan sedikitnya empat yurisdiksi kelembagaan yakni Kepolisian Republik Indonesia (selaku penyidik tindak pidana asal dan TPPU), Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) sebagai lembaga intelijen keuangan, Otoritas Jasa Keuangan (OJK) sebagai otoritas pengawas sistem perbankan, serta Kejaksaan sebagai penuntut umum. mengilustrasikan penggunaan perusahaan cangkang (*shell companies*) yang memungkinkan pelaku mengendalikan dan melapisi aliran dana melalui struktur kepemilikan semu. Skema ini secara efektif menghambat identifikasi *beneficial owner* serta

menciptakan rangkaian transaksi yang tampak sah secara formal namun substansinya bertujuan menyembunyikan hasil kejahatan.[26]

Pola penyamaran aset tersebut semakin kompleks dengan meningkatnya penggunaan aset kripto sebagai sarana TPPU. Pelaku tidak lagi sekadar mentransfer aset kripto secara sederhana, tetapi menerapkan teknik lanjutan seperti *chain hopping* yakni perpindahan antar-blockchain dan pemanfaatan *mixers* atau *tumblers* untuk menghilangkan keterlacakan transaksi. Praktik ini merupakan bentuk *jurisdictional arbitrage* dan *technological arbitrage*, di mana pelaku secara sadar mengonversi aset dari kripto publik seperti Bitcoin ke *privacy coin* yang memiliki tingkat anonimitas tinggi, misalnya Monero, sebelum akhirnya dialihkan kembali ke *stablecoin* untuk dicairkan melalui bursa kripto di yurisdiksi dengan rezim *Know Your Customer* (KYC) dan *Anti-Money Laundering* (AML) yang lemah.[27]

Konstruksi modus tersebut menjadikan upaya pelacakan dan pemblokiran aset oleh aparat penegak hukum Indonesia sangat sulit dilakukan secara efektif. Kejahatan yang bersifat *borderless* ini berhadapan dengan mekanisme penegakan hukum yang secara normatif tetap dibatasi oleh prinsip teritorialitas, termasuk dalam tindakan penyitaan dan pemblokiran aset. Walaupun Indonesia telah memiliki kerangka kerja sama internasional seperti *Mutual Legal Assistance* (MLA)[28] serta PPATK memiliki kewenangan untuk mengajukan permintaan pemblokiran aset di luar negeri, mekanisme tersebut tidak mampu mengimbangi akselerasi transaksi kripto lintas negara.[29] Proses MLA yang memerlukan waktu berbulan-bulan kontras dengan kecepatan pelaku yang dapat memindahkan aset secara global hanya dalam hitungan menit. Kesenjangan kecepatan yang ekstrem ini menempatkan penegakan hukum pada posisi reaktif dan secara praktis menyebabkan negara hampir selalu kalah cepat dalam mencegah hilangnya atau berpindahnya aset hasil kejahatan.

[26] Pontoh, A. (2021). Tanggung jawab korporasi atas tindak pidana peretasan rekening nasabah bank. *Lex Privatum* , *6* (1).

[27] Gabrilia S. E. Lumingkewas. (2025). *Efektivitas Mutual Legal Assistance dalam Ekstradisi Kasus Kejahatan Transnasional*. *Lex Crimen, 13*(5). https://ejournal.unsrat.ac.id/v3/index.php/lexcrimen/article/view/64258/50612

[28] Saragih, J. T., Aditama, Y. L., & Siahaan, H. M. (2024). Effectiveness of Mutual Legal Assistance Treaty in Investigating Indonesian Kidney Sale Crimes in Cambodia. *Jurnal Ius Constituendum*, *9*(3), hal. 502

[29] Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK). (2023, 14 Desember). *Mengamankan hasil tindak pidana lintas batas negara: Implementasi regulasi tunda, henti dan blokir transaksi*. https://www.ppatk.go.id/news/read/1324/mengamankan-hasil-tindak-pidana-lintas-batas-negara-implementasi-regulasi-tunda-henti-dan-blokir-transaksi.html

KESIMPULAN

Berdasarkan analisis normatif dan studi kasus yang telah dipaparkan, penelitian ini menegaskan bahwa tindak pidana pembobolan rekening khususnya terhadap rekening dormant telah berkembang menjadi bentuk kejahatan terorganisir yang kompleks dan dapat dikualifikasikan sebagai *predicate crime* dalam tindak pidana pencucian uang. Namun, efektivitas penegakan hukum di Indonesia masih terkendala oleh kesenjangan antara perkembangan modus kejahatan siber yang sangat cepat dengan kapasitas regulasi, prosedur birokratis, serta keterbatasan kerangka kerja *Mutual Legal Assistance* (MLA) dalam menghadapi perpindahan aset lintas negara maupun konversi ke aset digital. Kasus pembobolan senilai Rp.204.000.000.000,- (Dua Ratus Empat Miliar Rupiah) memperlihatkan bahwa meskipun instrumen hukum seperti UU TPPU, UU ITE, dan UU PPSK telah tersedia, ketiadaan sistem peringatan dini antarbank serta rendahnya kapabilitas forensik digital menyebabkan respon penegakan hukum cenderung bersifat reaktif dan belum mampu meminimalkan kerugian nasabah secara optimal.

Penulis merekomendasikan perlunya reformasi hukum dan penguatan kelembagaan yang diarahkan pada harmonisasi regulasi yang secara tegas menghubungkan pembobolan rekening dengan mekanisme pencucian uang, serta penerapan standar *follow the money* yang adaptif terhadap teknologi, termasuk aset kripto. Penguatan koordinasi melalui integrasi data secara real time antara Polri, PPATK, OJK, dan industri perbankan menjadi krusial untuk menghilangkan ego sektoral serta mempercepat penelusuran aliran dana. Selain itu, peningkatan kedudukan Laporan Hasil Analisis (LHA) PPATK dalam proses pembuktian dan modernisasi infrastruktur keamanan siber perbankan juga diperlukan untuk menutup celah kerentanan sistem keuangan.

DAFTAR PUSTAKA

Buku

Malayu S. P. Hasibuan, Dasar-Dasar Perbankan, PT. Bumi Aksara, Jakarta, 2001.

Jurnal

Afifah, E. F. N., Simatangkir, D. W. E., & Faliha, N. S. (2025). Keamanan Siber Dalam Perbankan Serta Tantangan Dan Solusi Di Era Digital. *Jurnal Multidisiplin Ilmu Akademik*, *2*(1).

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, *5*(02).

Almira Qurrotul Aini and Elanti Fatayatun Khoiroh. (2024). Perlindungan Hukum Nasabah Dalam Kasus Pembobolan Rekening Bank Di Indonesia. *Jurnal Multidisiplin Ilmu Akademik* 1(6).

Balaka, KI, Hakim, AR, & Sulistyany, FD (2024). Pencurian Informasi Nasabah di Sektor Perbankan: Ancaman Serius di Era Digital. *Justitiabelen* , *10* (2).

Dermawan, I., Baidawi, A., & Dewi, S. M. (2023). Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia. *Jurnal Informasi Dan Teknologi*, *5*(3).

Firzatul Rima Fitriana and Nuryanto A Daim. (2025). Peran PPATK Dalam Mengungkap Tindak Pidana Pencucian Uang Hasil Dari Tindak Pidana Korupsi. *Law and Humanity* 3(2).

Gabrilia S. E. Lumingkewas. (2025). *Efektivitas Mutual Legal Assistance dalam Ekstradisi Kasus Kejahatan Transnasional*. *Lex Crimen, 13*(5).

Judijanto, L., & Nugroho, B. (2025). Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrime di Indonesia. *Sanskara Hukum dan HAM*, *3*(03).

Khudsiyah, D., Rahmadan, D., & Erdianto, E. (2025). Penegakan Hukum Terhadap Modus Baru Kejahatan Cyber Berupa Rekayasa Informasi Teknologi Pembobolan Rekening Nasabah Melalui Internet Banking. *Jurnal Ilmiah Wahana Pendidikan*, *11*(8.D).

Luthfah, D. (2024). Penguatan Keamanan Siber Pada Sektor Jasa Keuangan Indonesia. *Jurnal Penelitian Dan Karya Ilmiah Lembaga Penelitian Universitas Trisakti*, *9*.

Meyrara Widya Putri and Jefry Tarantang. (2025). Optimalisasi Regulasi Perbankan Untuk Mempercepat Transformasi Digital Di Indonesia. *Belom Bahadat: Jurnal Hukum Agama Hindu* 15(1).

Pelupessy, B. E. (2025). Terobosan Hukum Dalam Rahasia Bank. *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial*, *2*(7), hal. 62-63

Pontoh, A. (2021). Tanggung jawab korporasi atas tindak pidana peretasan rekening nasabah bank. *Lex Privatum* , *6* (1).

Saragih, J. T., Aditama, Y. L., & Siahaan, H. M. (2024). Effectiveness of Mutual Legal Assistance Treaty in Investigating Indonesian Kidney Sale Crimes in Cambodia. *Jurnal Ius Constituendum*, *9*(3).

Internet

Burhan, F. A. (2023, Maret 9). *Industri finansial banjir serangan siber, bank digital pasang kuda-kuda*. Bisnis.com. https://finansial.bisnis.com/read/20230309/90/1635655/industri-finansial-banjir-serangan-siber-bank-digital-pasang-kuda-kuda

Humas Polri. *Bareskrim Polri ungkap sindikat pembobolan rekening dormant senilai Rp204 miliar, 9 tersangka diamankan*. https://humas.polri.go.id/news/detail/2102172-bareskrim-polri-ungkap-sindikat-pembobolan-rekening-dormant-senilai-rp204-miliar-9-tersangka-diam

Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), "Bareskrim Polri Ungkap Kasus Pembobolan Rekening Dorman Bank BUMN Rp204 Miliar Terkait Kejahatan Siber dan Pencucian Uang," *ppatk.go.id*, 23 Februari 2024, diakses 10 November 2025, https://www.ppatk.go.id/news/read/1529/bareskrim-polri-ungkap-kasus-pembobolan-rekening-dorman-bank-bumn-rp204-miliar-terkait-kejahatan-siber-dan-pencucian-uang.html.

Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK). (2023, 14 Desember). *Mengamankan hasil tindak pidana lintas batas negara: Implementasi regulasi tunda, henti dan blokir transaksi*. https://www.ppatk.go.id/news/read/1324/mengamankan-hasil-tindak-pidana-lintas-batas-negara-implementasi-regulasi-tunda-henti-dan-blokir-transaksi.html

Pusat Pelaporan dan Analisis Transaksi Keuangan. (2023, July 26). *Inffast*. https://www.ppatk.go.id/news/read/1278/inffast

Pusat Pelaporan dan Analisis Transaksi Keuangan. (n.d.). *Bareskrim Polri ungkap kasus pembobolan rekening Dorman Bank (BUMN) Rp 204 miliar terkait kejahatan siber dan pencucian uang*. https://www.ppatk.go.id/news/read/1529/bareskrim-polri-ungkap-kasus-pembobolan-rekening-dorman-bank-bumn-rp204-miliar-terkait-kejahatan-siber-dan-pencucian-uang.html

Pusat Pelaporan dan Analisis Transaksi Keuangan. 2025. Bareskrim Polri Ungkap Kasus Pembobolan Rekening Dorman Bank BUMN Rp204 Miliar, Terkait Kejahatan Siber dan Pencucian Uang. Diakses pada 30 Oktober 2025 dari https://www.ppatk.go.id/news/read/1529/bareskrim-polri-ungkap-kasus-pembobolan-rekening-dorman-bank-bumn-rp204-miliar-terkait-kejahatan-siber-dan-pencucian-uang.html

Puslit & BK DPR RI. (2025, September). *Isu Sepekan – IV: Pengungkapan sindikat pembobol rekening dormant* (No. 2046). https://berkas.dpr.go.id/pusaka/files/isu_sepekan/Isu%20Sepekan---IV-PUSLIT-September-2025-2046.pdf

Siti Yona Hukmana. Ini *peran 9 tersangka pembobol rekening dormant bank pemerintah senilai Rp204 miliar*. MetroTV News. https://www.metrotvnews.com/read/NleC8v78-ini-peran-9-tersangka-pembobol-rekening-dormant-bank-pemerintah-senilai-rp204-miliar