NEXUS RESEARCH PUBLISHING

Nexus of Justitia Law Review
Volume 1, Number 2, 2026
E-ISSN : 3124-0860
Open Access: https://journal.nexuspublishing.co.id/njlr

Akses Ilegal dan Phising pada Platform Cryptocurrency: Perspektif KUHP Baru dan UU ITE

Mutiara Oktoviani [1], Ayu Aryunah [2], Pira Ratnasari [3] Novita Lumban Batu[4], Bagus Ridho Pribadi[5]
[1] Fakultas Hukum Universitas Pamulang Serang Banten Indonesia
[2] Fakultas Hukum Universitas Pamulang Serang Banten Indonesia
[3] Fakultas Hukum Universitas Pamulang Serang Banten Indonesia
[4] Fakultas Hukum Universitas Pamulang Serang Banten Indonesia
[5] Fakultas Hukum Universitas Pamulang Serang Banten Indonesia
Correspondence: mutiaraoktoviani53@gmail.com

mutiaraoktoviani53@gmail.com [1], ayuaryunah8@gmail.com[2], piraratnasari00@gmail.com[3]
nnovitalumbanbatu@gmail.com[4], bagus300800@gmail.com[5]

Article Info

Article history:
Received th, 2026
Revised th, 2026
Accepted Nov 26th, 2026

Keyword:
Akses ilegal;
Phising; *Cryptocurrency*;
KUHP Baru;
UU ITE

ABSTRACT (10 PT)

Perkembangan teknologi keuangan digital telah melahirkan aset kripto (*cryptocurrency*) sebagai inovasi dalam sistem keuangan global. Namun, pesatnya adopsi aset kripto di Indonesia yang menduduki peringkat ketiga pasar kripto dunia tidak diimbangi dengan kesiapan sistem hukum nasional dalam menangani kejahatan siber yang menyertainya, khususnya akses ilegal melalui metode *phising* pada platform transaksi digital. Artikel ini bertujuan untuk menganalisis pengaturan tindak pidana akses ilegal dengan metode *phising* pada platform *cryptocurrency* dalam perspektif Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Kitab Undang-Undang Hukum Pidana baru (UU No. 1 Tahun 2023).

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan studi kasus terhadap putusan pengadilan terkait. Hasil penelitian menunjukkan bahwa ketentuan mengenai akses ilegal dalam UU ITE yang diatur dalam Pasal 30 jo. Pasal 46 telah dicabut dan direformulasi ke dalam Pasal 332 KUHP baru dengan sistematika yang lebih efisien karena menggabungkan rumusan perbuatan dan ancaman pidana dalam satu pasal. Namun, penegakan hukum menghadapi tantangan signifikan berupa status hukum kripto yang ambigu sebagai komoditas menurut Bappebti namun bukan alat pembayaran sah menurut Bank Indonesia serta keterbatasan kapasitas teknis aparat penegak hukum dalam pelacakan aset digital. Artikel ini merekomendasikan perlunya harmonisasi regulasi dan peningkatan kapasitas *digital forensik* aparat penegak hukum.

© 2026 The Authors. Published by PT Nexus Research Publishing. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang semakin masif telah mengubah lanskap kehidupan manusia secara fundamental, khususnya dalam sektor ekonomi dan keuangan. Inovasi digital tidak hanya mempermudah akses terhadap layanan keuangan, tetapi juga melahirkan produk-produk baru yang sebelumnya tidak terbayangkan, salah satunya adalah aset kripto (*cryptocurrency*) (Nakamoto:2008). Sebagai mata uang digital yang beroperasi berbasis teknologi *blockchain* dan dimanfaatkan melalui platform transaksi digital, *cryptocurrency* menawarkan sejumlah keunggulan, antara lain kecepatan transaksi lintas batas negara, biaya yang relatif rendah, serta sifatnya yang terdesentralisasi tanpa keterlibatan perantara lembaga keuangan tradisional (Swan:2015). Namun demikian, di sisi lain, arakteristik *cryptocurrency* yang bersifat anonim, tidak terikat pada yurisdiksi negara tertentu, dan sulit dilacak menjadikannya rentan terhadap penyalahgunaan untuk berbagai

kejahatan siber, termasuk akses ilegal melalui metode *phising* (Bambauer:2018; Irwan dan Haryanto:2021).

Fenomena kejahatan siber di Indonesia menunjukkan peningkatan yang sangat signifikan dalam dekade terakhir. Berdasarkan data yang dirilis oleh Pusat Informasi Kriminal Nasional Bareskrim Polri, kasus kejahatan siber di Indonesia mengalami lonjakan tajam dari 8.636 perkara pada tahun 2022 menjadi 13.913 perkara pada tahun 2024 (Bareskrim Polri:2024). Angka ini belum mencakup kasus-kasus yang tidak dilaporkan (*dark figure*) yang diperkirakan jauh lebih besar. Di antara berbagai modus kejahatan siber, *phising* menempati posisi sebagai salah satu modus operandi yang paling dominan dan merugikan masyarakat (Kominfo:2023). Metode *phising* dilakukan dengan mengirimkan tautan atau email palsu yang mengatasnamakan institusi terpercaya guna mengelabui korban agar memberikan informasi pribadi secara sukarela, seperti *username*, *password*, nomor kartu kredit, atau kode OTP (*One Time Password*) (Hadnagy:2011). Dalam konteks platform *cryptocurrency*, serangan *phising* menjadi ancaman yang sangat serius karena pelaku yang berhasil memperoleh kredensial akun korban dapat dengan mudah mentransfer aset digital ke dompet elektronik yang tidak terlacak, sehingga korban kehilangan asetnya secara permanen tanpa mekanisme pemulihan yang memadai (Irwan dan Haryanto:2021; Chainalysis:2022).

Indonesia saat ini tengah berada dalam fase transisi besar dalam kerangka hukum pidana siber. Pemberlakuan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP baru) membawa perubahan fundamental, salah satunya dengan mencabut ketentuan akses ilegal yang sebelumnya diatur dalam Pasal 30 juncto Pasal 46 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan mereformulasikannya ke dalam Pasal 332 KUHP baru (Parlambang Junior, Yuningsih dan Febriansyah:2026). Perubahan ini bukan sekadar pergeseran formal antarundang-undang, tetapi mengandung implikasi mendalam terhadap sistematika perumusan tindak pidana dan pendekatan penegakan hukum kejahatan siber di Indonesia (Ramadhan, Wahyudi dan Lbn Batu:2026).

KUHP baru mengintegrasikan rumusan perbuatan dan ancaman pidana dalam satu pasal yang lebih efisien, serta menggunakan sistem kategorisasi denda yang lebih fleksibel dibandingkan UU ITE yang bersifat absolut (Arief:2018). Namun demikian, terlepas dari perubahan regulasi tersebut, tantangan penegakan hukum di lapangan tetap kompleks, terutama berkaitan dengan status hukum *cryptocurrency* yang masih ambigu, keterbatasan kapasitas teknis aparat dalam melakukan pelacakan aset digital berbasis *blockchain*, serta belum terintegrasinya koordinasi antarlembaga penegak hukum (BRIN:2025; Mustapa:2025).

Berdasarkan latar belakang tersebut, artikel ini mengangkat tiga rumusan masalah utama. Pertama, bagaimana pengaturan akses ilegal melalui metode *phising* pada platform *cryptocurrency* dalam perspektif Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)? Kedua, bagaimana pengaturan akses ilegal tersebut dalam KUHP baru serta apa perbedaannya dengan pengaturan dalam UU ITE? Ketiga, apa saja tantangan penegakan hukum dalam kasus akses ilegal pada platform *cryptocurrency* di Indonesia? Ketiga rumusan masalah ini akan dikaji secara mendalam melalui pendekatan yuridis normatif guna memberikan pemahaman komprehensif mengenai kesiapan sistem hukum pidana Indonesia dalam menghadapi kejahatan siber di era ekonomi digital.

METODOLOGI

Penelitian ini menggunakan metode penelitian hukum normatif (*yuridis normatif*) sebagai pendekatan utama dalam mengkaji pengaturan akses ilegal melalui metode *phising* pada platform cryptocurrency berdasarkan perspektif Undang-Undang Informasi dan Transaksi Elektronik serta Kitab Undang-Undang Hukum Pidana baru (Marzuki:2017).

Penelitian hukum normatif merupakan penelitian yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagai bahan dasar untuk diteliti dengan cara mengkaji, menelaah, dan menginterpretasikan peraturan perundang-undangan, asas-asas hukum, serta doktrin hukum yang relevan dengan permasalahan yang diangkat (Soekanto dan Mamudji:2015). Pendekatan ini dipilih karena sesuai dengan karakteristik pokok permasalahan yang bersifat konseptual-regulatif, yakni

menyangkut pengaturan hukum positif tentang tindak pidana akses ilegal dan perubahannya dalam kerangka perundang-undangan nasional (Ali:2018).

Pendekatan yang digunakan dalam penelitian ini terdiri atas tiga pendekatan utama. Pertama, pendekatan perundang-undangan (*statute approach*) dilakukan dengan menelaah secara sistematis dan komprehensif ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, khususnya Pasal 30 juncto Pasal 46 yang mengatur tindak pidana akses ilegal, serta Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, khususnya Pasal 332 yang mereformulasi ketentuan akses ilegal dari UU ITE (Parlambang Junior, Yuningsih dan Febriansyah:2026).

Kedua, pendekatan kasus (*case approach*) dilakukan dengan menganalisis putusan-putusan pengadilan yang berkaitan dengan tindak pidana akses ilegal pada platform *cryptocurrency* (Marzuki:2017). Putusan-putusan tersebut dihimpun dari direktori putusan Mahkamah Agung Republik Indonesia melalui laman resmi putusan mahkamah agung dengan menggunakan kata kunci pencarian antara lain "akses ilegal", "*cryptocurrency*", "*phising*", "UU ITE", dan "Pasal 332 KUHP" untuk periode 2020-2025. Pendekatan kasus digunakan untuk mengetahui bagaimana penerapan hukum oleh hakim dalam praktik peradilan (*judicial practice*) serta untuk mengidentifikasi pola penafsiran hukum yang berkembang dalam menangani kasus-kasus serupa (Soekanto dan Mamudji:2015). Dari hasil penelusuran, ditemukan beberapa putusan yang relevan, salah satunya adalah Putusan Pengadilan Negeri Pekanbaru Nomor 764/Pid.Sus/2022/PN.Pbr yang secara eksplisit mengadili kasus akses ilegal ke akun Coinbase dengan metode *phising*. Analisis terhadap putusan ini dilakukan dengan menelaah pertimbangan hukum (*ratio decidendi*) majelis hakim, terutama dalam mengkonstruksikan unsur-unsur tindak pidana dan pembuktian barang bukti digital (Atmasasmita:2018).

Ketiga, pendekatan komparatif (*comparative approach*) digunakan untuk membandingkan pengaturan tindak pidana akses ilegal antara UU ITE dan KUHP baru, baik dari aspek substansi, sistematika, maupun ancaman pidana (Lamintang:2011). Pendekatan komparatif ini penting untuk mengidentifikasi perubahan-perubahan mendasar yang dibawa oleh KUHP baru serta implikasinya terhadap penegakan hukum kejahatan siber di Indonesia ke depan (Arief:2018). Dengan membandingkan kedua instrumen hukum tersebut, penelitian ini diharapkan dapat memberikan gambaran yang jelas mengenai kesinambungan dan perubahan paradigma hukum pidana siber nasional.

Bahan hukum yang digunakan dalam penelitian ini terdiri atas tiga jenis. Bahan hukum primer meliputi peraturan perundang-undangan yang mengikat dan memiliki kekuatan hukum tetap, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE, Undang-Undang Nomor 1 Tahun 2023 tentang KUHP, serta putusan-putusan pengadilan yang relevan dengan pokok permasalahan (Soekanto dan Mamudji:2015). Bahan hukum sekunder berupa literatur hukum, buku-buku teks, jurnal ilmiah, artikel hukum, dan hasil-hasil penelitian terdahulu yang membahas tentang tindak pidana akses ilegal, kejahatan siber, *cryptocurrency*, serta perbandingan antara UU ITE dan KUHP baru (Marzuki:2017). Sumber-sumber sekunder ini berfungsi untuk memberikan landasan teoretis dan konseptual bagi analisis bahan hukum primer. Bahan hukum tersier berupa kamus hukum, ensiklopedia, dan indeks kumulatif yang membantu peneliti dalam memahami istilah-istilah teknis yang digunakan dalam peraturan dan literatur hukum (Ali:2018).

Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*) dengan menginventarisasi, mengidentifikasi, dan mengkategorisasi seluruh bahan hukum yang relevan berdasarkan topik dan permasalahan penelitian (Soekanto dan Mamudji:2015). Seluruh bahan hukum yang terkumpul kemudian dianalisis secara kualitatif dengan menggunakan metode analisis yuridis normatif, yaitu suatu metode analisis yang menekankan pada penafsiran teks peraturan perundang-undangan dan putusan pengadilan serta menghubungkannya dengan konsep-konsep hukum dan doktrin yang berkembang (Marzuki:2017). Analisis dilakukan dengan langkah-langkah sebagai berikut: (1) identifikasi dan klasifikasi bahan hukum, (2) interpretasi dan sistematisasi bahan hukum, (3) penarikan kesimpulan secara deduktif dengan mendasarkan pada premis-premis hukum yang bersifat umum untuk

kemudian diterapkan pada kasus-kasus konkret yang dianalisis (Ali:2018). Pendekatan komparatif digunakan secara konsisten dalam proses analisis untuk membandingkan pengaturan akses ilegal antara UU ITE dan KUHP baru, sehingga dapat diidentifikasi perbedaan-perbedaan normatif beserta implikasi yuridisnya (Lamintang:2011).

Untuk menjamin validitas dan reliabilitas hasil penelitian, dilakukan triangulasi sumber bahan hukum, yaitu membandingkan dan mengkonsolidasikan berbagai bahan hukum primer, sekunder, dan tersier guna memperoleh pemahaman yang komprehensif dan menghindari kesimpulan yang parsial (Marzuki:2017). Selain itu, penelitian ini juga mengikuti kaidah-kaidah penulisan ilmiah yang baku dengan menyertakan sitasi yang jelas dan terpercaya dari setiap bahan hukum yang digunakan (Atmasasmita:2018).

HASIL DAN PEMBAHASAN

A. Pengaturan Akses Ilegal dan *Phising* dalam UU ITE

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) mengatur tindak pidana akses ilegal dalam Pasal 30 ayat (1), (2), dan (3) juncto Pasal 46 ayat (1), (2), dan (3). Pasal 30 ayat (1) UU ITE merumuskan bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun dipidana (Hukumonline:2024). Pasal 30 ayat (2) mengatur akses ilegal dengan tujuan memperoleh informasi elektronik dan/atau dokumen elektronik. Sementara itu, Pasal 30 ayat (3) mengatur akses ilegal dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan (Ramadhan, Wahyudi dan Lbn Batu:2026). Ketentuan ini mencerminkan upaya pembentuk undang-undang untuk memberikan perlindungan hukum terhadap sistem elektronik dan data digital di tengah pesatnya perkembangan teknologi informasi (Maskun:2013).

Ancaman pidana untuk ketiga tindak pidana tersebut diatur secara terpisah dalam Pasal 46 UU ITE, dengan pidana penjara paling lama 6 tahun untuk Pasal 30 ayat (1), 7 tahun untuk Pasal 30 ayat (2), dan 8 tahun untuk Pasal 30 ayat (3), serta denda masing-masing Rp600.000.000,00, Rp700.000.000,00, dan Rp800.000.000,00 (Ramadhan, Wahyudi dan Lbn Batu:2026). Selain itu, terdapat ketentuan pemberatan pidana dalam Pasal 52 UU ITE, di mana jika perbuatan akses ilegal ditujukan terhadap komputer atau sistem elektronik milik pemerintah atau yang digunakan untuk layanan publik, maka pidana pokok ditambah sepertiga. Lebih berat lagi, jika tindak pidana tersebut ditujukan terhadap komputer atau sistem elektronik milik pemerintah dan/atau badan strategis termasuk lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, atau otoritas penerbangan ancaman pidananya ditambah dua-pertiga (Hukumonline:2024). Demikian pula, jika tindak pidana dilakukan oleh korporasi, pidana pokok ditambah dua-pertiga (Hartono:2014). Ketentuan pemberatan ini menunjukkan keseriusan negara dalam melindungi infrastruktur kritis dari serangan siber (Maskun:2013).

Dalam konteks kasus akses ilegal pada platform *cryptocurrency*, putusan pengadilan menunjukkan bahwa metode *phising* termasuk dalam kategori menjebol sistem pengamanan sebagaimana dimaksud Pasal 30 ayat (3) UU ITE. Dalam Putusan Nomor 764/Pid.Sus/2022/PN.Pbr, terdakwa terbukti melakukan akses ilegal ke akun Coinbase milik korban dengan metode *phising* melalui email palsu yang mengatasnamakan pihak platform (Putusan PN Pekanbaru:2022). Terdakwa berhasil memperoleh kode OTP melalui akses ke email korban dan menggunakannya untuk masuk ke akun Coinbase korban. Fakta persidangan mengungkap bahwa terdakwa membeli daftar satu juta email calon korban seharga Rp300.000, SMTP (*Simple Mail Transfer Protocol*) seharga Rp150.000, serta memperoleh aplikasi *sender* dan *validator* secara gratis dari berbagai akun Facebook untuk melancarkan aksinya (Putusan PN Pekanbaru:2022). Terdakwa bahkan mempelajari cara melakukan *phishing* secara otodidak melalui *YouTube* sebelum melancarkan aksinya (Kejaksaan Agung:2025).

Majelis hakim menyatakan bahwa perbuatan terdakwa memenuhi unsur Pasal 30 ayat (3) UU ITE karena terdakwa berhasil menjebol sistem pengamanan akun Coinbase dan email korban. Selain itu, perbuatan terdakwa juga memenuhi unsur Pasal 32 ayat (1) UU ITE tentang transmisi informasi elektronik secara melawan hukum karena terdakwa melakukan transmisi kode OTP dari akun Coinbase

ke email korban (Putusan PN Pekanbaru:2022). Kerugian yang dialami korban seorang warga negara asing berdomisili di New Hampshire, Amerika Serikat mencapai sekitar 148 ETH (*Ethereum*) atau setara dengan Rp6.522.123.080 pada saat eksekusi putusan (Kejaksaan Agung:2025). Terdakwa berhasil menarik dana hasil kejahatan melalui rekening Bank BTPN dan Bank BCA miliknya sebanyak 31 kali dengan nilai bervariasi hingga total Rp16,5 miliar (Kejaksaan Agung:2025). Kasus ini menunjukkan bahwa akses ilegal melalui *phising* tidak hanya merugikan individu tetapi juga memiliki dimensi lintas negara yang kompleks.

B. Pengaturan Akses Ilegal dan *Phising* dalam KUHP Baru

Undang-Undang Nomor 1 Tahun 2023 tentang KUHP secara tegas mencabut ketentuan Pasal 30 dan Pasal 46 UU ITE yang mengatur akses ilegal dan intersepsi (Parlambang Junior, Yuningsih dan Febriansyah:2026). Pencabutan ini tidak menimbulkan kekosongan hukum (*rechtsvacuum*) karena materi muatan tersebut direformulasi dan dikodifikasi ke dalam Pasal 332 KUHP baru sebagai bagian dari tindak pidana terhadap informatika dan elektronika (Ramadhan, Wahyudi dan Lbn Batu:2026). Langkah kodifikasi ini merupakan bagian dari upaya harmonisasi hukum pidana nasional yang selama ini tersebar dalam berbagai undang-undang khusus (Arief:2018).

Pasal 332 KUHP baru merumuskan tiga jenis tindak pidana akses ilegal. Ayat (1) mengatur akses ilegal tanpa tujuan tertentu dengan pidana penjara paling lama 6 tahun atau denda kategori V (maksimal Rp500.000.000) (Pikiran Rakyat:2022). Ayat (2) mengatur akses ilegal dengan tujuan memperoleh informasi elektronik/dokumen elektronik dengan pidana penjara paling lama 7 tahun atau denda kategori V (maksimal Rp500.000.000). Ayat (3) mengatur akses ilegal dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dengan pidana penjara paling lama 8 tahun atau denda kategori VI (maksimal Rp2.000.000.000) (Pikiran Rakyat:2022; RMGuard:2025). Perbedaan signifikan terletak pada besaran denda maksimal UU ITE menetapkan denda maksimal Rp800.000.000 untuk akses ilegal dengan menjebol sistem pengamanan, sedangkan KUHP baru menetapkan denda kategori VI sebesar Rp2.000.000.000 (Jurnal Aktual Justice:2024). Hal ini menunjukkan peningkatan efek jera dari sisi denda, meskipun ancaman pidana penjara tetap sama.

Perbedaan mendasar antara UU ITE dan KUHP baru terletak pada sistematika perumusan. UU ITE memisahkan rumusan perbuatan dalam Pasal 30 dan ancaman pidana dalam Pasal 46, sedangkan KUHP baru menggabungkan rumusan perbuatan, perilaku, akibat, dan sanksi pidana dalam satu pasal, sehingga lebih efisien (Ramadhan, Wahyudi dan Lbn Batu:2026). Namun, materi muatan substantif tentang unsur-unsur tindak pidana akses ilegal tetap sama, yaitu adanya unsur kesengajaan, tanpa hak atau melawan hukum, dan akses terhadap komputer/sistem elektronik (Parlambang Junior, Yuningsih dan Febriansyah:2026). Hal ini penting untuk menjaga kepastian hukum dan kesinambungan penegakan hukum di tengah perubahan regulasi.

C. Perbandingan Pengaturan dan Implikasinya

Perbandingan pengaturan akses ilegal antara UU ITE dan KUHP baru menunjukkan beberapa aspek penting. Pertama, dari segi ancaman pidana, KUHP baru menggunakan sistem kategorisasi denda yang lebih fleksibel. Denda kategori V dalam KUHP baru diatur dalam Pasal 79 dengan besaran yang dapat disesuaikan melalui peraturan pemerintah, sedangkan UU ITE menetapkan besaran denda secara absolut (Ramadhan, Wahyudi dan Lbn Batu:2026). Sistem kategorisasi ini memberikan ruang bagi penyesuaian nilai denda terhadap perkembangan ekonomi tanpa harus mengubah undang-undang (Arief:2018).

Kedua, KUHP baru menghapus ketentuan tentang intersepsi atau penyadapan yang sebelumnya juga diatur dalam UU ITE. Hal ini menunjukkan adanya penyederhanaan dan pengelompokan tindak pidana siber secara lebih sistematis, meskipun sebagian pihak mengkhawatirkan adanya kekosongan pengaturan untuk tindak pidana penyadapan yang tidak termasuk dalam akses ilegal (Ramadhan, Wahyudi dan Lbn Batu:2026). Namun, pencabutan ini juga dapat dimaknai sebagai upaya untuk menghindari tumpang tindih pengaturan dengan instrumen hukum lainnya, seperti Undang-Undang tentang Penyelenggaraan Sistem Elektronik dan peraturan sektoral lainnya.

Ketiga, dari perspektif penegakan hukum, pencabutan ketentuan akses ilegal dari UU ITE dan pemindahannya ke KUHP baru memiliki implikasi terhadap harmonisasi hukum pidana. Dengan

terintegrasinya ketentuan ini ke dalam KUHP, maka tindak pidana akses ilegal menjadi bagian dari sistem hukum pidana nasional yang lebih komprehensif dan tidak lagi tersebar dalam berbagai undang-undang khusus (Parlambang Junior, Yuningsih dan Febriansyah:2026). Hal ini memudahkan aparat penegak hukum dalam merujuk pada satu sumber hukum yang terpadu, serta memungkinkan diterapkannya ketentuan umum KUHP, seperti percobaan, penyertaan, dan pemidanaan, secara lebih konsisten.

D. Tantangan Penegakan Hukum Akses Ilegal pada Platform *Cryptocurrency*

Meskipun kerangka hukum telah tersedia, penegakan hukum terhadap akses ilegal pada platform *cryptocurrency* menghadapi tantangan yang signifikan. Penelitian Badan Riset dan Inovasi Nasional (BRIN) mengungkap setidaknya tiga hambatan utama: ambiguitas status hukum *cryptocurrency*, keterbatasan kapasitas teknis aparat, dan koordinasi antarlembaga yang belum terintegrasi (BRIN:2025).

Pertama, ambiguitas status hukum *cryptocurrency* di Indonesia. Bank Indonesia melarang penggunaan kripto sebagai alat pembayaran berdasarkan Undang-Undang Nomor 7 Tahun 2011 tentang Mata Uang untuk menjaga kedaulatan Rupiah, sedangkan Bappebti melegitimasi kripto sebagai komoditas berjangka yang dapat diperdagangkan secara sah di bursa berjangka (Studi Regulasi Bitcoin:2026). Dualisme ini menimbulkan kebingungan dalam penanganan kasus, karena kripto sering kali hanya dipandang sebagai sarana dalam tindak pidana, bukan elemen sentral yang juga perlu diproses secara hukum (Mustapa:2025). Perubahan signifikan terjadi pada Januari 2025 ketika pengawasan aset kripto beralih dari Bappebti ke Otoritas Jasa Keuangan (OJK) berdasarkan Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK) (ANTARA:2025). Peralihan ini bertujuan untuk memberikan kepastian hukum dan penguatan sektor keuangan digital, namun hingga saat ini harmonisasi regulasi antarlembaga masih menjadi tantangan (Studi Regulasi Bitcoin:2026). OJK mencatat terdapat 21,70 juta akun konsumen aset keuangan digital dan aset kripto di Indonesia pada April 2026, yang menunjukkan besarnya pasar dan urgensi pengaturan yang jelas (Pintu Academy:2026).

Kedua, keterbatasan kapasitas teknis aparat penegak hukum. Sifat desentralisasi dan anonimitas transaksi kripto menyulitkan pelacakan aset digital. Aparat penegak hukum mengakui adanya kesenjangan kompetensi antara pelaku kejahatan yang semakin canggih dengan kemampuan penegak hukum dalam melakukan pelacakan aset berbasis *blockchain* (BRIN:2025). Metode *digital forensik* masih belum familiar bagi sebagian aparat, padahal pendekatan ini dinilai paling efektif untuk menelusuri portofolio aset digital (Mustapa:2025). Asosiasi Blockchain Indonesia (ABI) menyelenggarakan forum Bulan Literasi Kripto–Aparat Penegak Hukum (BLK APH) pada Mei 2026 untuk memperkecil celah antara inovasi teknologi aset digital yang pesat dan kesiapan penegakan hukum di Indonesia (Media Indonesia:2026). Forum ini melibatkan OJK, KPK, PPATK, Satgas PASTI, UNODC, Polda Metro Jaya, dan Bareskrim Polri dalam upaya menciptakan solusi bersama (Tribunnews:2026; Suara Karya:2026). Seperti dinyatakan Wakil Sekretaris Jenderal ABI, "Realitas yang kita hadapi bukan lagi soal hitam atau putih. Munculnya berbagai laporan mengenai kerugian masyarakat atau aliran dana yang sulit terlacak adalah konsekuensi dari adanya jarak antara kecepatan inovasi dan kesiapan perangkat pendukungnya" (Media Indonesia:2026).

Ketiga, koordinasi antarlembaga yang belum terintegrasi. Proses penegakan hukum sering tersendat pada tahapan penelusuran dompet aset digital karena belum adanya pedoman yang seragam di kepolisian, kejaksaan, dan lembaga peradilan. Saat ini, baru Kejaksaan yang telah memiliki pedoman khusus terkait penanganan kasus kripto (BRIN:2025). Namun, dalam kasus Putusan Nomor 764/Pid.Sus/2022/PN.Pbr, kolaborasi antara Kejaksaan Negeri Pekanbaru, Biro Hukum dan Hubungan Luar Negeri Kejaksaan Agung, Kedutaan Besar Amerika Serikat di Jakarta, dan Bank BRI menunjukkan bahwa koordinasi antarlembaga dapat berjalan efektif dalam eksekusi restitusi lintas negara (Kejaksaan Agung:2025). Hal ini menjadi preseden positif bagi penanganan kasus serupa di masa depan.

Selain itu, kasus pembobolan rekening Indodax yang viral pada tahun 2025 menunjukkan bahwa *phishing* dan *malware* menjadi modus utama akses ilegal ke akun pengguna. Otoritas Jasa Keuangan (OJK) yang kini menjadi pengawas aset kripto telah memanggil manajemen Indodax untuk

menelusuri kasus tersebut, namun proses pembuktian dan penyitaan aset digital masih menghadapi kendala teknis yang kompleks. OJK juga diberi kewenangan baru untuk membekukan atau menghentikan transaksi dan aktivitas perdagangan aset kripto jika ditemukan indikasi masalah (Pintu Academy:2026).

E. Relevansi Perubahan Regulasi terhadap Penanganan Kasus

Perubahan regulasi dari UU ITE ke KUHP baru tidak secara otomatis menyelesaikan tantangan penegakan hukum yang bersifat teknis dan prosedural. Sebagaimana diidentifikasi dalam berbagai penelitian, kelemahan utama terletak pada ketiadaan aturan khusus mengenai *cryptocurrency* yang menyulitkan pembuktian unsur pidana dan penyitaan aset digital (BRIN:2025; Mustapa:2025). KUHP baru yang masih bersifat umum dalam mengatur tindak pidana akses ilegal belum mengakomodasi karakteristik khusus aset digital seperti *cryptocurrency* (Ramadhan, Wahyudi dan Lbn Batu:2026). Kitab Undang-Undang Hukum Acara Pidana (KUHAP) yang masih berorientasi pada barang bukti konvensional juga belum mengakomodasi karakteristik aset digital, sehingga penyitaan dan perampasan aset kripto sering kali menimbulkan perbedaan pandangan dan gugatan praperadilan (Parlambang Junior, Yuningsih dan Febriansyah:2026).

Oleh karena itu, diperlukan pengaturan yang lebih komprehensif mengenai penyitaan aset digital, peningkatan kapasitas teknis aparat penegak hukum, klarifikasi kewenangan antarlembaga, serta integrasi mekanisme nasional dengan standar internasional seperti FATF (*Financial Action Task Force*) dan Konvensi Budapest tentang Kejahatan Siber (Mustapa:2025; Studi Regulasi Bitcoin:2026). Sebagaimana diusulkan dalam berbagai kajian, pembentukan Undang-Undang Aset Digital Nasional sebagai *lex specialis* yang mengintegrasikan fungsi pengawasan moneter, perdagangan, dan keuangan, serta pembentukan badan koordinasi seperti *National Crypto Regulatory Board* (NCRB), diperlukan untuk menciptakan sistem hukum aset digital yang terpadu dan adaptif terhadap perkembangan teknologi (Studi Regulasi Bitcoin:2026). Tanpa langkah-langkah tersebut, kesenjangan antara inovasi teknologi dan kesiapan hukum akan terus menjadi celah yang dieksploitasi oleh pelaku kejahatan siber (ABI:2026).

KESIMPULAN

Pengaturan akses ilegal melalui metode *phising* pada platform *cryptocurrency* di Indonesia telah mengalami perubahan signifikan dengan diberlakukannya KUHP baru (UU No. 1 Tahun 2023). Ketentuan akses ilegal yang sebelumnya diatur secara terpisah dalam Pasal 30 juncto Pasal 46 UU ITE dicabut dan direformulasi ke dalam Pasal 332 KUHP baru (Ramadhan, Wahyudi dan Lbn Batu:2026). Secara substantif, unsur-unsur tindak pidana tetap sama, yaitu adanya unsur kesengajaan, tanpa hak atau melawan hukum, dan akses terhadap komputer/sistem elektronik (Parlambang Junior, Yuningsih dan Febriansyah:2026). Namun, sistematika perumusan dalam KUHP baru lebih efisien karena menggabungkan rumusan perbuatan, perilaku, akibat, dan ancaman pidana dalam satu pasal, berbeda dengan UU ITE yang memisahkan rumusan perbuatan dan ancaman pidana dalam pasal yang terpisah (Ramadhan, Wahyudi dan Lbn Batu:2026). Selain itu, KUHP baru menerapkan sistem kategorisasi denda yang lebih fleksibel dengan denda kategori VI maksimal Rp2.000.000.000 untuk akses ilegal dengan menjebol sistem pengamanan, jauh lebih tinggi dibandingkan denda absolut Rp800.000.000 dalam UU ITE (Pikiran Rakyat:2022; Jurnal Aktual Justice:2024).

Praktik peradilan menunjukkan bahwa metode *phising* pada platform *cryptocurrency* termasuk dalam kategori menjebol sistem pengamanan sebagaimana dimaksud Pasal 30 ayat (3) UU ITE, sebagaimana dibuktikan dalam Putusan Nomor 764/Pid.Sus/2022/PN.Pbr yang mengadili kasus akses ilegal ke akun Coinbase dengan kerugian mencapai Rp6,5 miliar (Putusan PN Pekanbaru:2022; Kejaksaan Agung:2025). Perubahan regulasi dari UU ITE ke KUHP baru menandai langkah harmonisasi hukum pidana nasional dengan mengkodifikasikan ketentuan akses ilegal ke dalam KUHP, sehingga tidak lagi tersebar dalam berbagai undang-undang khusus (Arief:2018).

Meskipun kerangka hukum pidana materiil telah tersedia, penegakan hukum terhadap akses ilegal pada platform *cryptocurrency* menghadapi tantangan signifikan berupa ambiguitas status hukum kripto yang masih mengalami dualisme pengawasan antara Bank Indonesia dan Bappebti, meskipun telah terjadi peralihan pengawasan aset kripto ke OJK berdasarkan UU P2SK (BRIN:2025;

ANTARA:2025; Studi Regulasi Bitcoin:2026). Tantangan berikutnya adalah keterbatasan kapasitas teknis aparat dalam *digital forensik* berbasis *blockchain*, yang mulai direspons melalui forum BLK APH yang diselenggarakan Asosiasi Blockchain Indonesia pada Mei 2026 (Media Indonesia:2026; Tribunnews:2026). Hambatan ketiga adalah belum terintegrasinya koordinasi antarlembaga penegak hukum dalam penelusuran dompet aset digital, meskipun Kejaksaan telah memiliki pedoman khusus dan berhasil menunjukkan kolaborasi efektif dalam eksekusi restitusi lintas negara pada kasus PN Pekanbaru (BRIN:2025; Kejaksaan Agung:2025). Hambatan prosedural seperti penyitaan aset digital juga belum terakomodasi secara memadai dalam KUHAP yang masih berorientasi pada barang bukti konvensional, sehingga penyitaan dan perampasan aset kripto sering menimbulkan perbedaan pandangan dan gugatan praperadilan (Parlambang Junior, Yuningsih dan Febriansyah:2026; Mustapa:2025).

DAFTAR PUSTAKA

Ali, Zainuddin. (2018). *Metode Penelitian Hukum*. Jakarta: Sinar Grafika.

ANTARA News. (2025). Bappebti Fokus di PBK Setelah Pengawasan Aset Kripto di OJK dan BI. 11 September 2025.

Arief, Barda Nawawi. (2018). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana*. Jakarta: Prenada Media.

Atmasasmita, Romli. (2018). *Reformasi Hukum, Hak Asasi Manusia dan Penegakan Hukum*. Bandung: Refika Aditama.

Badan Riset dan Inovasi Nasional (BRIN). (2025). *Kajian Kesiapan Sistem Hukum Indonesia dalam Menghadapi Kejahatan Aset Kripto*. Jakarta: BRIN Press.

Bambauer, Derek. (2018). Cryptocurrency and Criminal Law. Dalam Markus D. Dubber dan Tatjana Hörnle (Ed.), *The Oxford Handbook of Criminal Law* (hlm. 789-812). Oxford: Oxford University Press.

Bareskrim Polri. (2024). *Laporan Tahunan Pusat Informasi Kriminal Nasional (Pusiknas): Perkembangan Kejahatan Siber di Indonesia 2022-2024*. Jakarta: Divisi Humas Polri.

Bisnis.com. (2026). Viral Rekening di Indodax Bobol, OJK Beberkan Perkembangan Kasusnya. 2 Januari 2026.

Chainalysis. (2022). *The 2022 Crypto Crime Report*. New York: Chainalysis Inc.

Hadnagy, Christopher. (2011). *Social Engineering: The Art of Human Hacking*. Indianapolis: Wiley Publishing.

Hartono, Bambang. (2014). Hacker dalam Perspektif Hukum Indonesia. *Jurnal MMH*, 43(1).

Hukumonline. (2024). Bunyi Pasal 30 Ayat (1) UU ITE tentang Peretasan. 9 Januari 2024.

International Telecommunication Union. (2012). *Understanding Cybercrime, Phenomena, Challenges, and Legal Response*. Switzerland: Geneva.

Irwan, Rizal dan Dedy Haryanto. (2021). Perlindungan Hukum bagi Pengguna Cryptocurrency dari Kejahatan Phising di Indonesia. *Jurnal Hukum dan Teknologi*, 9(2), 145-162.

Jurnal Aktual Justice. (2024). Perbandingan Pengaturan Akses Ilegal dalam UU ITE dan KUHP Baru. *Jurnal Aktual Justice*, 9(2).

Kejaksaan Agung Republik Indonesia. (2025). Kejati Riau Eksekusi Restitusi WNA Korban Phising Senilai Rp6,5 Miliar dari Pelaku yang Tak Tamat SD. *Story Kejaksaan*, 26 Mei 2025.

Kementerian Komunikasi dan Informatika. (2023). *Laporan Tahapan Penanganan Kejahatan Siber dan Modus Phising di Indonesia*. Jakarta: Direktorat Jenderal Aptika Kominfo.

Kompas.com. (2023). Aturan Akses Ilegal dan Penyadapan dalam KUHP Baru. 5 Maret 2023.

Lamintang, P.A.F. (2011). *Dasar-Dasar Hukum Pidana Indonesia*. Bandung: PT. Citra Aditya Bakti.

Marzuki, Peter Mahmud. (2017). *Penelitian Hukum: Edisi Revisi*. Jakarta: Kencana Prenada Media Group.

Maskun. (2013). *Kejahatan Siber (Cyber Crime) Suatu Pengantar*. Jakarta: Kencana.

Media Indonesia. (2026). Pertumbuhan Aset Kripto dan Teknologi Blockchain Jadi Tantangan Aparat Penegak Hukum. 8 Mei 2026.

Mustapa, Erni. (2025). Penegakan Hukum Terhadap Tindak Pidana Pencucian Uang dalam Kasus Cyber Transaksi Kripto Ilegal. *Lex Crimen*, 14(3), 89-104.

Nakamoto, Satoshi. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf.

Parlambang Junior, Muhammad Daffa, Henny Yuningsih, dan Artha Febriansyah. (2026). The Urgency of Regulation of Money Laundering Criminal Acts Through Cryptocurrency Methods in Indonesia. *Jurnal Inovasi Pembangunan*, 14(1), 55-72.

Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 5 Tahun 2019 tentang Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto (Crypto Asset) di Bursa Berjangka.

Pikiran Rakyat. (2022). KUHP Baru: Hack Orang Lain Dipenjara Sampai 8 Tahun atau Denda hingga Rp2 Miliar. 7 Desember 2022.

Pintu Academy. (2026). Panduan Lengkap Regulasi Aset Crypto di Indonesia 2026. 14 Juli 2026.

Putusan Pengadilan Negeri Pekanbaru Nomor 764/Pid.Sus/2022/PN.Pbr.

Ramadhan, Taufiq, Arief Wahyudi, dan Dewi Pika Lbn Batu. (2026). Illegal Access Melalui Metode Phising Pada Platform Transaksi Digital Cryptocurrency Dalam Perspektif KUHP Baru dan Undang-Undang ITE. *PAGARUYUANG Law Journal*, 9(2), 210-235.

RMGuard. (2025). KUHP UU Nomor 1 Tahun 2023 [Bagian 4]. 8 Desember 2025.

RRI.co.id. (2025). BRIN Sebut Sistem Hukum Indonesia Belum Siap Kripto. 28 November 2025.

Soekanto, Soerjono dan Sri Mamudji. (2015). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Pers.

Studi Regulasi Bitcoin. (2026). Legal Status of Bitcoin in Indonesia: Regulatory Synchronization Challenges. *Garuda-Garba Rujukan Digital*.

Suara Karya. (2026). Asosiasi Blockchain Indonesia Dorong Sinergi Aparat Penegak Hukum Perkuat Keamanan Ekosistem Kripto Nasional. 9 Mei 2026.

Swan, Melanie. (2015). *Blockchain: Blueprint for a New Economy*. Sebastopol: O'Reilly Media.

Tribunnews. (2026). ABI Gelar Forum Literasi Kripto untuk Aparat Penegak Hukum, Bahas Tantangan Aset Digital. 13 Mei 2026.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952).

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842).