PAGARUYUANG Law Journal
Volume 9 No. 2, Januari 2026
P-ISSN: 2580-4227, E-ISSN: 2580-698X

PLaJ. *Faculty of law* Universitas Muhammadiyah Sumatera Barat, Indonesia.
Open Acces at: https://jurnal.umsb.ac.id/index.php/pagaruyuang

Illegal Access Melalui Metode *Phising* Pada *Platform* Transaksi Digital *Cryptocurrency* Dalam Perspektif KUHP Baru dan Undang-Undang ITE

Taufiq Ramadhan, Arief Wahyudi, & Dewi Pika Lbn Batu

Program Studi Hukum Bisnis Fakultas Ilmu Sosial Universitas Negeri Medan
Jurusan PPKN Fakultas Ilmu Sosial Universitas Negeri Medan
Email: taufiqramadhan@unimed.ac.id, ariefwahyudi@unimed.ac.id, & dewi_pika_lumban@unimed.ac.id

Abstract

Indonesia is one of the countries experiencing an emergency in terms of cybercrime. This can be seen in the significant increase in cybercrime cases released by the National Police Criminal Investigation Center from 2022 to 2025. One type of crime is illegal access through the phishing method on the cryptocurrency digital transaction platform. This research aims to analyze the various forms of phishing as a modus operandi used in committing crimes collected through the directory of supreme court decisions and analyze the actions in the perspective of the New Criminal Code and ITE Law. This case is interesting to be reviewed in depth through a comprehensive and normative legal analysis. Therefore, this research uses a qualitative method with a normative juridical approach. Based on the results of the research conducted, first, there are various forms and modes of phishing forms committed by perpetrators of illegal access crimes without rights compiled from the supreme court decision directory such as phishing through fake emails, phishing tool kits, phishing including malware viruses, cash phishing vandalism, and trap scripts. Second, in the perspective of the ITE Law, illegal access by phishing method is regulated in Article 30 paragraph (3) jo Article 46 paragraph (3) jo Article 36 paragraph (2) jo Article 51 paragraph (2). The legal material in the ITE Law separates the formulation of the article of criminal behavior, the consequences caused, the sanctions and the elements of the crime in contrast to Law Number 1 of 2023 concerning the Criminal Code (new Criminal Code) which is more efficient because in 1 article contains the formulation of actions, behavior, consequences and criminal sanctions at once. In the new Criminal Code, illegal access by phishing method is regulated in Article 332.

Keywords: *Phising, Cryptocurrency, New Criminal Code, Electronik Information and Transaction Law*

Abstrak

Indonesia menjadi salah satu negara yang mengalami keadaan darurat dalam hal kejahatan siber. Hal ini terlihat pada peningkatan yang signifikan kasus kejahatan siber yang dirilis oleh Pusiknas Bareskrim Polri Tahun 2022 hingga 2025. Salah satu jenis kejahatannya adalah akses ilegal melalui metode phising pada plaltform transaksi digital cruptocurrency. Penelitian ini bertujuan untuk menganalisis berbagai bentuk phising sebagai modus operandi yang digunakan dalam melakukan kejahatan yang dihimpun melalui direktori putusan mahkamah agung dan menganalisis perbuatannya dalam perspektif KUHP Baru dan UU ITE. Kasus ini menarik untuk diulas secara mendalam melalui analisis hukum yang komprehensif dan bersifat normatif. Oleh karena itu penelitian ini menggunakan metode kualitatif dengan jenis pendekatan yuridis normatif. Berdasarkan hasil penelitian yang dilakukan, pertama terdapat berbagai bentuk dan modus operandi phising yang dilakukan oleh pelaku kejahatan akses ilegal

sebagaimana dihimpun dari direktori putusan mahkamah agung yaitu phising melalui email palsu, phising tool kit, phising menyertakan virus malware, vandalisme cash phising, dan script jebakan. Kedua, dalam perspektif Undang-Undang ITE, akses ilegal dengan metode phising yang menimbulkan kerugian diatur dalam Pasal 30 ayat (3) jo. Pasal 46 ayat (3) jo. Pasal 36 ayat (2) jo. Pasal 51 ayat 2. Materi hukum dalam Undang-undang Informasi dan Transaksi Elektronik (UU ITE) memisahkan rumusan pasal perilaku kejahatan, akibat yang ditimbulkan, sanksi dan unsur-unsur kejahatannya berbeda dengan Undang-undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP baru) yang lebih efisien karena dalam 1 pasal mengandung rumusan perbuatan, perilaku, akibat dan sanksi pidana sekaligus. Dalam KUHP baru, akses ilegal dengan metode phising diatur pada Pasal 332.

Kata Kunci: *Akses Ilegal, Phising, Cryptocurrency, KUHP Baru, Hukum ITE*

A. PENDAHULUAN

Perkembangan teknologi saat ini diibaratkan pisau yang bermata dua, satu sisi memberikan dampak positif seperti mudahnya akses informasi secara digital, sisi lainnya memberikan dampak negatif seperti pencurian data pribadi, data akun (*username* dan *password)*, dan data finansial seperti informasi kartu debit, kartu kredit dan rekening lainnya [1]. Berbagai modus operandi yang dilakukan oleh pelaku untuk mencuri dan mengakses informasi secara ilegal seperti metode *phising*.

Phising berasal dari kata *Fishing* yaitu memancing atau mencari ikan (korban) dengan menggunakan umpan palsu atau manipulatif. Metode yang umum digunakan oleh pelaku dengan mengirimkan jebakan link/tautan dan email yang berisi informasi palsu [2] . Hal ini dilakukan sebagai upaya untuk mengelabui korban dengan tujuan agar memberikan informasi pribadi secara sukarela tanpa kesadaran bahwa korban telah diperdaya dan mencuri secara langsung data kredensial akun transaksi digital korbannya. Informasi yang didapatkan oleh pelaku digunakan tanpa hak dan melawan hukum untuk mengakses secara ilegal data akun yang dimiliki korbannya.

Saat ini, Indonesia menjadi salah satu negara yang darurat dalam hal kejahatan di dunia maya atau yang kerap disebut dengan kejahatan siber (*cyber Crime*). Berdasarkan data yang dirilis oleh Pusat Informasi Kriminal Nasional Badan Reserse Kriminal Polri bahwa terjadi peningkatan yang signifikan terhadap kasus kejahatan siber terhitung dari tahun 2022 sampai dengan awal tahun 2025. Jumah kasus pada tahun 2022 adalah 8.636 perkara, Tahun 2023 berjumlah 11.297 perkara dan Tahun 2024 mencapai angka

[1] Clara Nervia et al., "Analisis Yuridis Terhadap Kejahatan Phising Dalam Sistem Perbankan Digital Melalui Scam" 29, no. 2 (2025): 13–30.

[2] Devi Puspitasari and Tata Sutabri, "Analisis Kejahatan Phising Pada Sektor E-Commerce Di Marketplace Shopee," *Jurnal Digital Teknologi Informasi* 6, no. 2 (2023): 76–81, https://doi.org/10.32502/digital.v6i2.5653.

13.913 Perkara [3]. Sementara terhitung sejak tanggal 01 sampai dengan 23 Januari Tahun 2025 jumlah kejahatan siber telah berada pada angka 1.062 kasus dengan jumlah orang yang ditindak sebagai terlapor kasus kejahatan tersebut berjumlah 32.000 terlapor. Dari jumlah kasus tersebut, pencurian data melalui metode *phising* menjadi salah satu jenis kejahatan siber yang telah ditangani oleh Polri.

Pencurian data akun yang dilakukan melalui metode *phising* misalnya pada akun *cryptocurrecy. Cryptocurrency* atau yang dikenal dengan aset kripto merupakan mata uang digital dan alat tukar uang yang penggunaannya melalui *platform* transaksi digital[4]. Sebagaimana daftar penyelenggara perdagangan aset keuangan digital yang telah dirilis oleh Otoritas Jasa Keuangan pada Maret 2025, *platform* transaksi digital yang dimaksud seperti Tokocrypto, Pluang, Mobee, Indodax, Pintu, Kriptosukses, dan Naga Exchange. Transaksi yang dilakukan pada *platform* mata uang digital ini terlindungi oleh kode pengaman informasi atau sandi rahasia yang dikenal dengan kriptografi. Penggunaan kriptografi sebagai pengaman ditujukan agar tidak terjadi alih fungsi/pemindahtanganan dan akses secara ilegal. Dalam beberapa kasus, keamanan dengan penggunaan teknologi kriptografi masih dapat dijebol oleh pihak yang tidak bertanggungjawab melalui pengelabuan dan pemberian informasi palsu yang dikirimkan ke email individu sebagai korbannya dan melalui link yang membuat korban sangat mudah sekali untuk diperdaya.

Tindakan akses ilegal melalui metode *phising* terhadap akun *cryptocurrecy* dilakukan melalui berbagai bentuk dan skenario yang tersusun secara rapi agar korbannya percaya dan tidak menyadari bahwa sedang diperdaya oleh pelaku. Fakta kasus yang terjadi pada penelitian ini berada pada Putusan Nomor 764/Pid.Sus/2022/PN.Pekan Baru. Dalam putusan ini, pelaku mengambil *User* ID dan password *coinbase* milik korban kemudian melakukan akses pada akun *coinbase cryptocurrency* dengan mata uang digital *etherium* (Eth) senilai $350.000 dan $100.000 untuk di *withdraw* ke rekening Bank milik korban yang telah terdaftar di akun *coinbase*

[3] Bareskrim Polri, "Tim Siber Ungkap Teknologi Deepfake Catut Nama Pejabat Negara," Pusat Informasi Kriminal Nasional Badan Reserse Kriminal Kepolisian Negara Republik Indonesia, 2025, https://pusiknas.polri.go.id/detail_artikel/tim_siber_ungkap_teknologi_deepfake_catut_nama_pejabat_negara.

[4] Bambang Arianto and Rani, *Penyusunan State of The Art Penelitian* (Balikpapan: Borneo Novelty Publishing, 2024).

namun ternyata telah dikonversi ke *etherium* dan sudah dilakukan transfer/pemindahan ke *wallet* kripto milik pelaku.

Fokus utama penelitian ini membahas tentang bentuk *phising* sebagai metode yang dilakukan untuk mengakses secara ilegal *platform* transaksi digital misalnya pada akun investasi *cryptocurrency* yang dihimpun dalam Direktori Putusan Mahkamah Agung dan perspektif KUHP baru & UU ITE dalam akses ilegal (*illegal access*) melalui metode *phising* pada akun *cryptocurrency*.

> Berdasarkan pengamatan yang dilakukan terkait dengan *state of the art* sekaligus mengidentifikasi kesenjangan terhadap penelitian sebelumnya bahwa ditemukan kebaharuan atau *novelty* dalam penelitian ini. Pengidentifikasian *state of the art* bertujuan untuk kebaharuan dan menghindari pengulangan terhadap penelitian yang telah ada sebelumnya[5].

Dalam hal substansial, penelitian ini membahas tentang akses ilegal dengan metode *phising* pada akun mata uang digital *cryptocurrency* dan bentuk *phising* sebagai metode yang dilakukan untuk mengakses *platform* digital secara ilegal yang dihimpun melalui direktori putusan mahkamah agung. Sementara beberapa penelitian terdahulu seperti penelitian oleh Irma Yurita pada Jurnal Hukum Legalita Tahun 2023 hanya membahas tentang pengaruh metode *phising* sebagai ancaman digital tanpa membahas bentuk-bentuk *phising* sebagai metode yang dilakukan untuk mengakses *plaform* digital secara ilegal berdasarkan fenomena dan fakta Putusan Pengadilan yang telah berkekuatan hukum tetap. Selanjutnya penelitian oleh I Kadek Odie Kharisma Putra pada Jurnal *Cyber Security* yang membahas *phising* sebagai kejahatan siber tanpa menentukan secara khusus *locus delicti* atau tempat dimana terjadinya tindak pidana kejahatan siber seperti *platform* digital, penelitian ini juga tidak melibatkan reformulasi hukum pada Kitab Undang-Undang Hukum Pidana baru.

B. METODE PENELITIAN

Kejahatan akses ilegal pada *platform* transaksi digital *cryptocurrency* merupakan fenomena sosial yang menarik untuk diulas secara mendalam melalui analisis hukum yang komprehensif dan bersifat normatif. Oleh karena itu, penelitian ini menggunakan metode kualitatif dengan jenis pendekatan yuridis normatif. Pemilihan metode

[5] Arianto and Rani.

kualitatif pada objek dan subjek penelitian ini didasarkan pada fundamen penting yang mengarahkan pendalaman analisis secara objektif dan memberikan wadah eksplorasi menyeluruh terhadap konsep hukum serta perspektif yang lebih holistik terhadap kedudukan hukum didalam masyarakat [6]. Pendekatan ini bertujuan untuk mengimplementasikan prinsip hukum normatif yang berfokus pada ketersediaan bahan hukum primer seperti peraturan perundang-undangan yang relevan, putusan pengadilan dan produk hukum lainnya, bahan hukum sekunder seperti buku referensi, serta bahan hukum tersier seperti kamus hukum dan ensiklopedia hukum. Penelitian yang dilakukan dengan pendekatan yuridis normatif dikatakan juga sebagai penelitian kepustakaan (*library research*) [7].

Analisis yang dilakukan bertujuan untuk mendeskripsikan secara jelas mengenai apa yang akan dituju dan dihasilkan dalam penelitian. Sebagaimana pendapat Cresswell bahwa tujuan penelitian bukanlah masalah yang dirumuskan namun maksud dan sasaran yang berhasil untuk diwujudkan [8]. Penelitian ini bertujuan untuk menganalisis berbagai bentuk *phising* sebagai modus operandi yang digunakan untuk mengakses secara ilegal *platform* transaksi digital *cryptocurrency* dan menganalisis perbuatannya dalam perspektif KUHP Baru dan Undang-Undang ITE.

C. HASIL DAN PEMBAHASAN

1. Bentuk *Phising* sebagai Metode yang dilakukan untuk Mengakses Secara Ilegal *Platform* Transaksi Digital

Illegal Access merupakan kejahatan transnasional yang dilakukan dengan berbagai tipe, bentuk dan modus operandi yang beraneka ragam. Menurut *International Telecommunication Union* atau yang dikenal dengan ITU bahwa terdapat berbagai tipe kejahatan siber sebagai kejahatan yang bertujuan untuk mencuri informasi komputer untuk mendapatkan keuntungan seperti tipe kejahatan kerahasiaan, komputer

[6] Tiyas Vika Widyastuti, Achmad Irwan Hamzani, and Fajar Dian Aryani, *Metodologi Penelitian Dan Penulisan Bidang Ilmu Hukum: Teori Dan Praktek* (Medan: PT. Media Penerbit Indonesia, 2024).

[7] Taufiq Ramadhan and Dewi Pika Lbn Batu, "Pertanggungjawaban Pidana Pelaku Pencabulan Terhadap Anak Yang Dilakukan Oleh Anak Ditinjau Dari Undang-Undang Perlindungan Anak & Sistem Peradilan Pidana Anak," *Ius Civile: Refleksi Penegakan Hukum Dan Keadilan* 7, no. 1 (2023): 23, https://doi.org/10.35308/jic.v7i1.7057.

[8] Nur Solikin, *Pengantar Metodologi Penelitian Hukum* (Pasuruan: CV. Penerbit Qiara Media, 2021).

dijadikan sebagai tempat berbuat kejahatan, kejahatan atas konten yang diunggah, dan kejahatan yang berkaitan dengan hak cipta [9].

> Berdasarkan tipe kejahatan siber yang dikemukakan oleh ITU, akses ilegal berada pada tipe kejahatan kerahasiaan. Kejahatan ini dilakukan dengan cara mengakses secara ilegal atau tanpa hak sistem komputer melalui berbagai metode seperti penyadapan komunikasi (*illegal interception*), intervensi data (*data interference*), gangguan sistem komputer melalui penyebaran virus (*system interference*), mencuri informasi penting seperti data pribadi, data akun dan data financial (*illegal data acquisition/data espionage*) [10].

Mengingat bahwa kejahatan siber dilakukan oleh pihak yang memiliki pemahaman dalam akses dan pengelolaan sistem komputer maka dalam proses penegakan hukumnya tidak dapat dilakukan dengan cara yang tradisional, dibutuhkan keterlibatan kemampuan teknologi elektronik yang canggih dan sumber daya yang khusus dan mumpuni untuk menyelesaikan masalah.

Ditemukan berbagai teknik dan cara untuk dapat menerobos sistem komputer secara ilegal, salah satunya dengan mengelabui dan memancing korbannya agar pelaku dapat mengakses secara ilegal *platform* akun transaksi digital yang kemudian merampas dan memindahkan saldo atau uang digital tersebut ke *wallet* pelaku. Berdasarkan eksplorasi dan analisis yang dilakukan pada berbagai putusan di direktori putusan mahkamah agung, maka didapati berbagai bentuk *phising* yang dilakukan oleh pelaku kejahatan dihimpun pada tabel dibawah ini :

Tabel 1. Data Bentuk *Phising* dan *Modus Operandi*

No	Aplikasi/ Platform Transaksi Digital	Bentuk Phising	Modus Operandi/Sumber Putusan
1.	Aplikasi *Cryptocurrency Coinbase*	Email Palsu	Mengirimkan email berisi informasi palsu dengan menggunakan *Sender* SMTP. Korban diminta untuk melakukan verifikasi dengan mengirimkan identitas data pribadi dan mengunjungi *website* palsu yang dibuat oleh pelaku. Korban diperdaya untuk *log-in* dan masuk kedalam *database db.txt*

[9] I Made Pasek Diantha and I Gede Pasek Eka Wisanjaya, *Analisis Kejahatan Transnasional Dalam Berbagai Instrumen Hukum Internasional* (Jakarta: Prenada Media, 2023).

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

			pelaku. (Putusan Nomor 764/Pid.Sus/2022/PN.Pekan Baru)
2.	PayPal, Apple, Amazon dan Kartu Kredit	*Phising* Tool Kit	Pelaku mengirim email berisi informasi palsu dengan tujuan untuk mencuri data pribadi, informasi akun dan data financial melalui *website* 16.shop. (Putusan Nomor 85/Pid.Sus/2022/PN.Bjb)
3.	Mandiri Internet	*Phising* menyertakan Virus *Malware*	Mencuri/merekam data melalui PC/Laptop yang terinfeksi virus *malware*. Setelah data didapat, system korban akan *log out* secara otomatis dan pelaku dapat mengendalikan kemudian mengakses *platform* transaksi digital milik korban. Pelaku memindahkan dana rekening melalui perintah/pesan palsu dengan narasi "*please change token PIN*" atau *verifying* dan menampilkan sejumlah angka yang merupakan *challenge code*. Saat korban melakukan perubahan Token PIN berdasarkan perintah pelaku melalui *malware*, maka terjadilah transaksi transfer data ke rekening pelaku. (Putusan Nomor 100 K/Pdt.Sus-BPSK/2016)
4.	*Uninterruptible Power Supply Automated Teller Machine* (UPS ATM)	*Vandalisme Cash Phising*	Mencuri uang pada mesin tarik tunai dengan modus memasangkan alat kendali di belakang UPS mesin. Saat transaksi penarikan uang dilakukan, pelaku me-*reversal* menggunakan *remote* agar saldo tidak berkurang namun uang sudah berada ditangannya. (Putusan Nomor 473/Pid.B/2019/PN.Btm) & (Putusan Nomor 474/Pid.B/2019/PN.Btm)
5.	*Credit Card* (CC)	*Script* Jebakan	Mengelabui korban dengan mengirimkan *script* atau email jebakan dengan maksud untuk mendapatkan informasi dan dokumen elektronik berupa data *Credit Card* (CC). Kartu Kredit atau Credit Card (CC) didapat dari *hacker* atau *spammer* dengan cara mencuri. Pelaku membuat *web* palsu agar korbannya diperdaya untuk mengisi data pribadi sehingga *hacker* atau *spammer* bisa menggunakan kartu kredit untuk kebutuhan komersil. (Putusan Nomor 845/Pid.Sus/202/PT.SBY)

Sumber : Direktori Putusan Mahkamah Agung, 2025

Dalam kasus putusan yang dihimpun pada tabel diatas menunjukkan bahwa terdapat berbagai metode *phising* dan modus operandi yang dilakukan oleh pelaku kejahatan. Modus operandi yang dilakukan sebagai cara untuk melancarkan tindakan kejahatan dan erat relevansinya dengan penggunaan teknologi informasi berbasis digital seperti pada platform media sosial, *e-commerce*, transaksi perbankan dan *platform* mata uang digital seperti *cryptocurrency*.

> Modus operandi dalam kejahatan siber (*cybercrime*) disebut dengan *unauthorized Access to computer system and service* atau melakukan akses secara ilegal dan tanpa hak pada sistem komputer tanpa adanya persetujuan dari pemilik dan pihak yang memiliki wewenang untuk menguasai sistem tersebut [11].

Pelaku kejahatan akses ilegal menerobos dan menjebol kode keamanan melalui metode *phising* atau mengelabui korbannya dengan mengirimkan informasi palsu melalui email, *script* jebakan, merekam data melalui virus *malware* yang memperdaya korban secara sadar untuk menyerahkan data akun, data pribadi dan data finansial. Data tersebut dipergunakan untuk mengakses secara illegal platform transaksi digital korban dan memindahkan dana atau saldo ke wadah/*wallet* milik pelaku.

> Modus operandi *illegal access* dengan metode *phising* memiliki perbedaan yang signifikan dengan kejahatan pada umumnya, salah satu hal yang terlihat berbeda adalah tempat dimana tindakan kejahatan itu dilakukan yang dikenal dengan *Locus Delicti* [12].

Umumnya pada kejahatan konvensional, *locus delicti* dipandang berdasarkan tempat akibat dari tindakan kejahatan itu terjadi, tempat alat yang dipakai untuk melakukan tindak kejahatan, dan tempat melakukan kejahatan secara fisik. Sementara dalam kejahatan *illegal access* dengan metode *phising* dilakukan secara virtual melalui jaringan komputer dan acap kali melibatkan beberapa lokasi akses yang berbeda-beda, ini alasan mengapa kejahatan ini dianggap sebagai kejahatan transnasional yang dilakukan secara lintas batas dan membutuhkan penyelesaian yang komprehensif dan khusus dalam upaya pencegahan dan penegakan hukumnya. Dalam hukum acara pidana *cyber*, ruang lingkup lintas batas memerlukan kerjasama dan koordinasi

[11] Ervan Yudi Widyarto and Dita Kusuma Hapsari, "Analisis Modus Operandi Tindak Kejahatan Menggunakan Teknik Komunikasi Love Scam Sebagai Ancaman Pada Keamanan Sistem Informasi," *Syntax Idea* 4, no. 9 (2022): 1352, https://doi.org/10.36418/syntax-idea.v4i9.1959.

[12] Widyarto and Hapsari.

internasional yang serius dan tersistematis dibandingkan pada hukum acara pidana konvensional [13]. Hal ini mempertimbangkan bahwa kejahatan *cyber* terjadi secara universal melingkupi berbagai negara di dunia.

Putusan Nomor 764/Pid.Sus/2022/PN.Pekan Baru pada tabel diatas, secara khusus menjadi fokus pembahasan utama pada penelitian ini. Metode *Phising* yang dilakukan sebagai modus operandi yaitu mengirimkan email berisi informasi palsu dengan menggunakan Sender SMTP. Korban diminta untuk melakukan verifikasi dengan mengirimkan identitas data pribadi dan mengunjungi *website coinbase* palsu yang dibuat oleh pelaku. *Website coinbase* memiliki kemiripan pada *website* aslinya agar korban diperdaya untuk *log-in* dan data akunnya masuk kedalam database db.txt pelaku. Pelaku merampas akun *coinbase* dan men-*generate* kode OTP milik korban. Setelah itu, pelaku *log in* ke email untuk mendapatkan kode OTP tersebut dan bebas melakukan akses pada *website coinbase*. Pelaku memilih asset mata uang digital *etherium* pada akun *cryptocurrency* yang tercantum pada *website* https://coinbase.com dan melakukan pemindahan dana atau saldo pada akun *wallet etherium* milik pelaku di https://indodax.com. Tindak pidana ilegal akses dengan metode *phising* pada kasus yang dibahas pada penelitian ini telah tervalidasi menggunakan *tools sender* dengan tujuan untuk mendapatkan *username* dan *password* guna menguasai email dan akun *coinbase* milik korbannya.

2. Perspektif KUHP Baru dan UU ITE Dalam Akses Ilegal (*Illegal Access*) Melalui Metode *Phising* pada *Platform* Transaksi Digital *Cryptocurrency*

Sebelum lahirnya KUHP baru Tahun 2023, penggunaan dan pemanfaatan informasi dan transaksi elektronik diatur dalam Undang-undang Nomor 19 Tahun 2016 perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dalam UU ITE tahun 2016, ilegal akses dengan metode *phising* diatur pada Pasal 30 ayat (3), Pasal 36, Pasal 46 ayat (3), Pasal 51 ayat (2)[14]. Penerapan hukum pada kasus akses ilegal memiliki banyak kaitan antara 1 pasal dengan pasal lainnya. UU ITE

[13] Husamuddin et al., *Hukum Acara Pidana Dan Pidana Cyber*, Pertama (Medan: PT. Media Penerbit Indonesia, 2024).

[14] Kemensesneg RI, *Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elketronik* (Jakarta, 2024).

dalam rumusan pasalnya memisahkan rumusan tindak kejahatan pelaku, dengan akibat yang ditimbulkan, sanksi yang diberikan dan unsur-unsur kejahatan.

Sebagaimana putusan Nomor 764/Pid.Sus/2022/PN.Pbr yang menjadi contoh kasus dalam pembahasan penelitian ini, kesalahan (*schuld*) yang dilakukan adalah dengan sengaja melakukan akses tanpa hak dan melawan hukum *platform* transaksi digital *cryptocurrency* pada *website* https://coinbase.com melalui tipu daya, memancing dan mengelabui korbannya dengan metode *phising*. Perbuatan yang dilakukan oleh pelaku mengakibatkan kerugian terhadap korban berupa berpindahnya aset mata uang digital Ethereum pada *website* https://coinbase.com ke akun *wallet etherium* pelaku pada akun https://indodax.com. Jumlah kerugian yang dihadapi oleh korban sebesar Rp. 6.500.000.0000 (enam milyar lima ratus juta rupiah) [15].

Perbuatan pelaku yang dengan sengaja mengakses secara ilegal dan menimbulkan kerugian bagi pemilik akun *coinbase cryptocurrency* menunjukkan bahwa pelaku telah melengkapi unsur objektif dan subjektif dalam Pasal 30 ayat (3) jo Pasal 46 ayat (3) jo Pasal 36 ayat (2) jo Pasal 51 ayat 2 Undang-Undang Nomor 19 Tahun 2016 Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Terpenuhinya unsur pidana menjadi dasar pelaku untuk mempertanggungjawabkan tindakannya, sebagaimana pertimbangan hakim pada putusan tersebut bahwa selain kesalahan yang telah terbukti, pelaku juga dapat mampu bertanggungjawab dan tidak terdapat alasan pembenar dan pemaaf baginya untuk melakukan kejahatan tersebut. Atas kejahatan akses ilegal pada akun *coinbase cryptocurrency* pelaku diberikan sanksi pidana penjara selama 3 (tiga) tahun 4 (empat) bulan dan denda sebesar Rp. 2.000.000 (dua milyar rupiah) dengan ketentuan jika denda tidak diberikan maka pelaku mengganti dengan pidana kurungan selama 2 (dua) bulan. Pelaku terbukti melakukan tindakan dengan sengaja mengakses system komputer tanpa hak/ilegal dengan cara menerobos, menjebol dan melakukan serangan kriptografi pada sistem keamanan akun *coinbase cryptocurrency* dan menyebabkan kerugian bagi orang lain.

[15] Mahkamah Agung Republik Indonesia, Putusan Nomor 764/Pid.Sus/2022/PN.Pbr (2022).

Keberadaan KUHP baru tahun 2023 telah mencabut secara tegas materi hukum tentang akses ilegal pada UU ITE dan melakukan reformulasi materi hukum baru pada bagian kelima tentang tindak pidana informatika dan elektronika dalam hal penggunaan dan perusakan Informasi elektronik[16]. Reformulasi dilakukan memandang berbagai kelemahan dan mempertimbangkan perkembangan masyarakat. Pertumbuhan sosial, ekonomi dan teknologi menandakan konstruksi sosial masyarakat telah berkembang [17].

Hal ini menunjukkan bahwa reformulasi hukum harus bisa menjadi alat kendali masyarakat sejalan dengan konsep yang dipopulerkan oleh *Roscoe Pound* tentang *law as a tool of social engineering* guna terimplementasikannya tujuan nasional Indonesia yakni mewujudkan masyarakat yang sejahtera, adil, makmur dan tertib hukum sebagaimana yang tertera didalam Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Berbeda dengan UU ITE Tahun 2016 dan 2008, materi hukum tentang tindak pidana informatika dan elektronik pada Undang-undang KUHP tidak memisahkan antara perbuatan pelaku, akibat, unsur dan sanksinya dalam beberapa pasal, namun menggabungkannya menjadi satu pasal atau ayat. Hal ini membuat pengimplementasian hukum dalam tindak pidana akses ilegal atau penggunaan komputer dan sistem elektronik tanpa hak menjadi lebih efisien dan komprehensif.

Kitab Undang-undang hukum pidana tahun 2023 hanya memuat 2 paragraf yang berisi 4 rumusan pasal yaitu :

1. Pasal 332 berisi tentang tindak pidana dengan sengaja melakukan akses terhadap komputer dan sistem komputer secara ilegal (tanpa hak) melalui berbagai metode dan modus kejahatan untuk maksud memperoleh informasi dan dokumen elektronik. Metode dan modus operandi dalam tindak pidana ini berupa menerobos, melampaui dan menjebol sistem keamanan. Sanksi pidana yang diatur dalam pasal ini adalah pidana denda pada kategori V dan VI, serta pidana penjara sesuai dengan tindakan yang dilakukan dengan masa waktu maksimal 6 (enam) tahun untuk akses ilegal, 7 (tujuh) tahun untuk akses ilegal dengan tujuan tertentu, 10 (sepuluh) tahun untuk akses ilegal dengan menerobos sistem keamanan komputer dan sistem elektronik.
2. Pasal 333 berisi tentang tindak pidana tanpa hak dan melampaui kewenangannya menggunakan atau melakukan akses komputer dan sistem elektronik yang

[16] Kemensesneg RI, *Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana* (Jakarta, 2023).

[17] Agung Tri Wicaksono and Ikhsan Fatah Yasin, "Criminal Law Reformulation Through Omnibus Law as a Solution to Sectoral Cyber Protection," *Al-Jinayah : Jurnal Hukum Pidana Islam* 10, no. 2 (2024): 237–61, https://doi.org/10.15642/aj.2024.10.2.237-261.

dilindungi oleh negara dan masyarakat dengan berbagai modus operandi dan tujuan tertentu yang mengakibatkan sistem informasi, pertahanan, dan hubungan internasional menjadi terganggu. Akibat dari tindak pidana ini juga menimbulkan resiko berbahaya pada negara dan subjek hukum internasional serta rusaknya sistem elektronik negara. Sanksi pidana yang diatur dalam pasal ini adalah pidana penjara dengan masa waktu maksimal 7 (tujuh) tahun dan denda paling banyak kategori VI.

3. Pasal 334 berisi tentang tindak pidana melakukan akses komputer atau sistem elektronik secara ilegal, tanpa hak dan melampaui wewenangnya melalui berbagai macam modus operandi dengan maksud untuk memperoleh keuntungan atau informasi keuangan yang berasal dari lembaga perbankan dan keuangan. Sanksi pidana yang diatur dalam pasal ini adalah pidana penjara maksimal 10 (sepuluh) tahun dan denda paling banyak pada kategori VI.
4. Pasal 335 berisi tentang tindak pidana melakukan akses komputer atau sistem elektronik tanpa hak melalui modus operandi apapun dengan maksud dan tujuan untuk memiliki, mengubah, merusak dan menghilangkan informasi yang dirahasiakan oleh pemerintah. Sanksi pidana yang diatur dalam pasal ini adalah pidana penjara maksimal 12 (dua belah) tahun dan denda paling banyak pada kategori VII.

Tindak pidana ilegal akses melalui metode *phising* pada *paltform* transaksi digital *cryptocurrency* pada putusan Nomor 764/Pid.Sus/2022/PN.Pbr, apabila dianalisis dengan menggunakan KUHP baru Tahun 2023 maka pelaku kejahatan maka dijerat dengan Pasal 332 KUHP. Hal ini dikarenakan, pelaku mengakses sistem elektronik milik orang lain berupa akun *coinbase* pada *website* https://coinbase.com secara ilegal melalui modus mengelabui dan memancing korbannya seperti mengirimkan email yang berisi informasi palsu untuk menerobos dan menjebol keamanan kriptografi sebagai password dan kode rahasia pada *platform* transaksi digital tersebut. Untuk menentukan apakah tindakan pelaku merupakan tindak pidana atau bukan maka dilakukan analisis terkait unsur subjektif dan objektifnya, tindakan pelaku telah melengkapi unsur subjektif karena melakukan tindakan akses ilegal secara sengaja dan telah melengkapi unsur objektif karena timbulnya dampak dan akibat dari perbuatan pelaku terhadap korban berupa jebolnya keamanan kriptografi dan diperolehnya informasi elektronik oleh pelaku untuk mengakses secara ilegal sistem elektronik korbannya.

> Pentingnya penjabaran rumusan delik kedalam unsur-unsurnya bertujuan untuk memastikan apakah seseorang melakukan perbuatan yang memenuhi kriteria dalam delik yang diatur oleh undang-undang. Dalam hukum pidana, unsur dibagi

2, pertama unsur subjektif yang berhubungan dengan diri si pelaku, kedua unsur objekti yang berhubungan dengan keadaan-keadaannya [18].

Memandang bahwa Pasal 36 UU ITE merumuskan secara khusus tentang kerugian sebagai akibat dari tindakan akses ilegal seperti *platform* transaksi digital, sebenaranya KUHP juga mencantumkan unsur objektif ini didalam Pasal 334, namun unsur "memperoleh keuntungan dari lembaga keuangan dan lembaga perbankan" tidak dapat disamakan dengan memperoleh keuntungan dari *cryptocurrency. Crytocurrency* bukan bagian dari lembaga keuangan dan tidak dapat diberlakukan sebagai alat pembayaran atau transaksi yang resmi di Indonesia, kedudukannya hanya sebagai entitas bergerak namun tidak memiliki bentuk/wujud [19]. Lembaga keuangan seperti Ototitas Jasa keuangan (OJK) dan Bank Indonesia (BI) memberikan larangan kepada pengelola jasa keuangan lainnya untuk memberikan akses, sarana dan prasarana perdagangan aset kripto karena saat ini lembaga keuangan seperti OJK dan BI hanya menjadi alat kontrol terhadap aset kripto di Indonesia sebagaimana ketentuan Pasal 6 ayat (1) huruf e Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan [20]. Hal ini disebabkan karena *cryptocurrency* adalah aset investasi [21], sementara mata uang dan alat tukar yang sah di Indonesia menurut Undang-Undang Nomor 7 Tahun 2011 tentang mata uang adalah Rupiah [22]. Mata uang rupiah terdiri dari rupiah kertas dan rupiah logam dengan simbol mata uang ini adalah Rp (Rupiah).

C. PENUTUP

Perkembangan teknologi ibarat pisau yang bermata dua, satu sisi memberikan kemudahan akses digital, namun pada sisi lainnya memberikan perubahan buruk terhadap perilaku sosial masyarakat. Saat ini Indonesia mengalami keadaan darurat terhadap kejahatan siber karena selama 4 (empat) tahun terakhir, kasus kejahatan ini terus meningkat secara signifikan. Salah satu jenis kejahatan siber adalah akses ilegal

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

[19] Ade Rizki Saputra, "Potential of Crypto Assets as Loan Collateral in Indonesia," *Formosa Journal of Social Sciences (FJSS)* 2, no. 4 (2023): 693–700, https://doi.org/10.55927/fjss.v2i4.7450.

[20] Kemensesneg RI, "Undang-Undang Nomor 4 Tahun 2023 Tentang Pengembangan Dan Penguatan Sumber Keuangan" (2023).

[21] Muhammad Yusuf Thohir, "Cryptocurrency Dalam Yurisdikdi Pajak Indonesia," Kementerian Keuangan Direktorat Jenderal Pajak, 2024, https://www.pajak.go.id/index.php/id/artikel/cryptocurrency-dalam-yurisdiksi-pajak-indonesia#:~:text=Mata uang kripto memang bukan,pembayaran yang sah di Indonesia.

[22] Kementerian Hukum dan HAM, *Undang-Undang Nomor 7 Tahun 2011 Tentang Mata Uang* (Jakarta, 2011).

(*Illegal Access)* yang dilakukan dengan metode *phising* pada *platform* transaksi digital. Metode Phising/fishing dilakukan untuk memancing dan mengelabui seseorang guna mendapatkan informasi dokumen elektronik. Setelah mendapatkan informasi tersebut, pelaku kejahatan melakukan akses secara ilegal *platform* transaksi digital seperti *crtocurrency* dengan cara menjebol dan menerobos sistem keamanan kriptografi milik korbannya. Terdapat berbagai bentuk dan modus operandi *phising* yang dilakukan oleh pelaku kejahatan akses ilegal sebagaimana dihimpun dari direktori putusan mahkamah agung yaitu *phising* melalui email palsu, *phising tool kit, phising* menyertaka*n virus malware, vandalisme cash phising, dan script* jebakan.

Berdasarkan perspektif Undang-Undang ITE Tahun 2016 perubahan atas UU ITE Tahun 2008, akses ilegal dengan metode *phising* yang menimbulkan kerugian diatur dalam Pasal 30 ayat (3) jo. Pasal 46 ayat (3) jo. Pasal 36 ayat (2) jo. Pasal 51 ayat (2). Materi hukum didalam UU ITE memisahkan rumusan pasal perilaku kejahatan, akibat yang ditimbulkan, sanksi dan unsur-unsur kejahatannya berbeda dengan KUHP baru tahun 2023 yang lebih efisien karena dalam 1 pasal mengandung rumusan perbuatan, perilaku, akibat dan sanksi pidana sekaligus. Dalam KUHP baru, akses ilegal dengan metode *phising* diatur pada Pasal 332.

DAFTAR PUSTAKA

Buku:

Arianto, Bambang, and Rani. *Penyusunan State of The Art Penelitian*. Balikpapan: Borneo Novelty Publishing, 2024.

Diantha, I Made Pasek, and I Gede Pasek Eka Wisanjaya. *Analisis Kejahatan Transnasional Dalam Berbagai Instrumen Hukum Internasional*. Jakarta: Prenada Media, 2023.

Husamuddin, Sumardi Efendi, Syaibatul Hamdi, Ida Rahma, Benni Erick, Novi Heryanti, and FriwartiSri Dewi. *Hukum Acara Pidana Dan Pidana Cyber*. Pertama. Medan: PT. Media Penerbit Indonesia, 2024.

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

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

Mahkamah Agung Republik Indonesia. Putusan Nomor 764/Pid.Sus/2022/PN.Pbr (2022).

Nervia, Clara, Kresentia Aiko Wardhana, Pricilia Angel Sie, and Talitha Livia Talim. "Analisis yuridis terhadap kejahatan phising dalam sistem perbankan digital melalui scam" 29, no. 2 (2025): 13–30.

Puspitasari, Devi, and Tata Sutabri. "Analisis Kejahatan Phising Pada Sektor E-

Commerce Di Marketplace Shopee." *Jurnal Digital Teknologi Informasi* 6, no. 2 (2023): 76–81. https://doi.org/10.32502/digital.v6i2.5653.

Ramadhan, Taufiq, and Dewi Pika Lbn Batu. "Pertanggungjawaban Pidana Pelaku Pencabulan Terhadap Anak Yang Dilakukan Oleh Anak Ditinjau Dari Undang-Undang Perlindungan Anak & Sistem Peradilan Pidana Anak." *Ius Civile: Refleksi Penegakan Hukum Dan Keadilan* 7, no. 1 (2023): 23. https://doi.org/10.35308/jic.v7i1.7057.

Saputra, Ade Rizki. "*Potential of Crypto Assets as Loan Collateral in Indonesia*." *Formosa Journal of Social Sciences (FJSS)* 2, no. 4 (2023): 693–700. https://doi.org/10.55927/fjss.v2i4.7450.

Solikin, Nur. *Pengantar Metodologi Penelitian Hukum*. Pasuruan: CV. Penerbit Qiara Media, 2021.

Thohir, Muhammad Yusuf. "Cryptocurrency Dalam Yurisdikdi Pajak Indonesia." Kementerian Keuangan Direktorat Jenderal Pajak, 2024. https://www.pajak.go.id/index.php/id/artikel/cryptocurrency-dalam-yurisdiksi-pajak-indonesia#:~:text=Mata uang kripto memang bukan,pembayaran yang sah di Indonesia.

Wicaksono, Agung Tri, and Ikhsan Fatah Yasin. "*Criminal Law Reformulation Through Omnibus Law as a Solution to Sectoral Cyber Protection*." *Al-Jinayah : Jurnal Hukum Pidana Islam* 10, no. 2 (2024): 237–61. https://doi.org/10.15642/aj.2024.10.2.237-261.

Widyarto, Ervan Yudi, and Dita Kusuma Hapsari. "Analisis Modus Operandi Tindak Kejahatan Menggunakan Teknik Komunikasi Love Scam Sebagai Ancaman Pada Keamanan Sistem Informasi." *Syntax Idea* 4, no. 9 (2022): 1352. https://doi.org/10.36418/syntax-idea.v4i9.1959.

Widyastuti, Tiyas Vika, Achmad Irwan Hamzani, and Fajar Dian Aryani. *Metodologi Penelitian Dan Penulisan Bidang Ilmu Hukum: Teori Dan Praktek*. Medan: PT. Media Penerbit Indonesia, 2024.

Peraturan Perundang-undangan:

Kemensesneg RI. *Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana*. Jakarta, 2023.

———. *Undang-Undang Nomor 4 Tahun 2023 Tentang Pengembangan dan Penguatan Sumber Keuangan* (2023).

———. *Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elketronik*. Jakarta, 2024.

Kementerian Hukum dan HAM. *Undang-Undang Nomor 7 Tahun 2011 Tentang Mata Uang*. Jakarta, 2011.

Website:

Polri, Bareskrim. "Tim Siber Ungkap Teknologi Deepfake Catut Nama Pejabat Negara." Pusat Informasi Kriminal Nasional Badan Reserse Kriminal Kepolisian Negara Republik Indonesia, 2025. https://pusiknas.polri.go.id/detail_artikel/tim_siber_ungkap_teknologi_deepfake_catut_nama_pejabat_negara.