PESHUM : Jurnal Pendidikan, Sosial dan Humaniora
Vol.4, No.3, April 2025

Tindak Pidana Penipuan Dalam Transaksi Online Sebagai Kejahatan Terorganisir Dan Kaitannya Dengan Pencucian Uang

Richard Tommy Pantow
Magister Hukum Universitas Kristen Indonesia
E-mail: pantowrichard76@gmail.com

Article History:
Received: 01 April 2025
Revised: 15 April 2025
Accepted: 17 April 2025

Keywords: *Penipuan online, Kejahatan terorganisir, pencucian uang, Hukum siber, Transaksi digital.*

Abstract: *Perkembangan teknologi digital telah memberikan kemudahan dalam aktivitas ekonomi, namun juga membuka peluang bagi tindak pidana baru, salah satunya adalah penipuan dalam transaksi online. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis modus serta pola kejahatan penipuan online, menjelaskan keterlibatannya dalam kejahatan terorganisir, serta menganalisis kaitannya dengan praktik pencucian uang. Metode yang digunakan adalah penelitian yuridis normatif dengan pendekatan perundang-undangan dan konseptual, serta didukung dengan studi kasus dan data sekunder. Hasil penelitian menunjukkan bahwa penipuan online banyak dilakukan oleh jaringan terorganisir yang terstruktur dengan peran yang terdistribusi, di mana hasil kejahatan disamarkan melalui skema pencucian uang yang kompleks, baik melalui rekening pihak ketiga maupun transaksi digital lintas negara. Kompleksitas ini menuntut regulasi yang adaptif, peningkatan kapasitas aparat penegak hukum, serta edukasi menyeluruh kepada masyarakat untuk mencegah semakin meluasnya dampak kejahatan tersebut. Dengan pemahaman yang komprehensif, diharapkan strategi pemberantasan tindak pidana ini dapat dilakukan secara lebih efektif dan terintegrasi.*

PENDAHULUAN

Tindak pidana penipuan merupakan salah satu bentuk kejahatan yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP), khususnya Pasal 378, yang menyatakan bahwa "barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapus piutang diancam karena penipuan dengan pidana penjara paling lama empat tahun." (Purba et al., 2023). Namun, dengan berkembangnya teknologi informasi, modus penipuan juga mengalami transformasi, terutama dalam ranah digital.

Seiring dengan itu, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang telah diperbarui melalui Undang-Undang Nomor 19 Tahun 2016, memberikan landasan hukum untuk mengatur tindak pidana penipuan yang dilakukan

melalui media elektronik (Bastari et al., 2024). Pasal 28 ayat (1) UU ITE menyatakan bahwa "Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik." Ketentuan ini memberikan dasar hukum untuk menindak pelaku penipuan yang memanfaatkan teknologi informasi dalam melakukan aksinya.

Namun, terdapat tumpang tindih antara ketentuan dalam KUHP dan UU ITE terkait penipuan, yang dapat menimbulkan kebingungan dalam penegakan hukum. Asas lex specialis derogat legi generalis menyatakan bahwa hukum yang lebih khusus mengesampingkan hukum yang lebih umum. Dalam konteks ini, UU ITE sebagai hukum khusus seharusnya mengesampingkan KUHP dalam kasus penipuan yang dilakukan melalui media elektronik. Namun, dalam praktiknya, penerapan asas ini masih menghadapi tantangan, terutama dalam menentukan yurisdiksi dan kewenangan penegakan hukum (Astiti, 2024).

Kejahatan terorganisir merupakan bentuk kejahatan yang dilakukan oleh kelompok atau organisasi yang memiliki struktur dan hierarki tertentu, dengan tujuan untuk memperoleh keuntungan secara ilegal. (Siegel, 2020) mendefinisikan kejahatan terorganisir sebagai tindakan ilegal yang dijalankan oleh suatu jaringan terstruktur untuk mendapatkan profit melawan hukum. Karakteristik utama dari kejahatan terorganisir meliputi adanya perencanaan yang matang, pembagian peran yang jelas di antara anggota kelompok, serta penggunaan kekerasan atau ancaman untuk mencapai tujuan. Kejahatan terorganisir biasanya mencakup tiga unsur: organisasi kriminal yang kuat, jaringan pelindung, dan masyarakat penerima manfaat dari tindakan ilegal yang terstruktur (Hisyam et al., 2024). Dalam konteks penipuan online, kejahatan terorganisir dapat terwujud melalui sindikat yang terlibat dalam berbagai tahap penipuan, mulai dari perencanaan hingga pencucian uang.

Penipuan online yang dilakukan oleh kelompok terorganisir seringkali melibatkan jaringan yang luas, termasuk pelaku yang berada di luar negeri. Hal ini menyulitkan penegakan hukum, terutama dalam hal koordinasi lintas negara dan yurisdiksi. Selain itu, penggunaan teknologi canggih oleh pelaku, seperti enkripsi dan jaringan anonim, semakin mempersulit upaya penegakan hukum. Oleh karena itu, diperlukan kerja sama internasional yang erat dalam menangani kejahatan terorganisir yang melibatkan penipuan online.

Perkembangan teknologi informasi telah mengubah cara masyarakat bertransaksi, dengan meningkatnya penggunaan platform online untuk jual beli barang dan jasa. Teknologi yang berkembang cepat memegang peran penting dalam masyarakat, mempermudah pengelolaan informasi sehari-hari (Sari & Nasution, 2024). Namun, kemudahan ini juga dimanfaatkan oleh pelaku kejahatan untuk melakukan penipuan melalui media elektronik. Kejahatan siber (cybercrime) dalam konteks transaksi online mencakup berbagai modus, seperti phishing, spoofing, dan penggunaan situs palsu untuk menipu korban.

Kejahatan siber dalam transaksi online tidak hanya merugikan individu, tetapi juga dapat berdampak pada stabilitas ekonomi dan kepercayaan publik terhadap sistem digital. Dalam penelitian yang dilakukan oleh (Simbolon et al., 2021), disebutkan bahwa perdagangan berbasis sistem elektronik harus dilindungi keamanannya oleh pemerintah dengan melakukan koordinasi yang bersifat lini sektoral, perluasan kewenangan, dan membentuk beberapa kebijakan baru dalam pengamanan dan penindakan terhadap e-commerce.

Untuk mengatasi kejahatan siber dalam transaksi online, diperlukan pendekatan yang komprehensif, termasuk peningkatan literasi digital masyarakat, penguatan regulasi, serta pengembangan teknologi keamanan yang dapat mendeteksi dan mencegah aktivitas ilegal secara real-time. Selain itu, kerja sama antara sektor publik dan swasta juga penting dalam menciptakan ekosistem digital yang aman dan terpercaya.

PESHUM : Jurnal Pendidikan, Sosial dan Humaniora
Vol.4, No.3, April 2025

Pencucian uang merupakan proses menyamarkan asal-usul uang yang diperoleh dari kegiatan ilegal, sehingga tampak seolah-olah berasal dari sumber yang sah. Proses ini umumnya terdiri dari tiga tahap: placement (penempatan), layering (pelapisan), dan integration (penggabungan) (Mardiyati, 2022).. Dalam konteks penipuan online, hasil kejahatan seringkali dicuci melalui berbagai metode, seperti transfer antar rekening, penggunaan mata uang kripto, atau investasi dalam aset legal.

Modus pencucian uang yang terkait dengan penipuan online semakin kompleks, dengan pelaku memanfaatkan teknologi untuk menyembunyikan jejak transaksi. Penggunaan platform digital yang menawarkan anonimitas, seperti dompet digital dan mata uang kripto, mempersulit upaya pelacakan oleh otoritas. Selain itu, pelaku juga seringkali memanfaatkan identitas palsu atau rekening atas nama orang lain (nominee account) untuk mengaburkan asal-usul dana yang diperoleh dari kejahatan. Identitas tersebut bisa diperoleh melalui pencurian data pribadi (identity theft) atau hasil kerja sama dengan pihak ketiga yang turut terlibat dalam jaringan kejahatan. Hal ini menimbulkan tantangan besar bagi lembaga pengawas keuangan dan aparat penegak hukum dalam menelusuri aliran dana ilegal yang tersebar dalam berbagai rekening dan platform digital secara simultan.

Dalam beberapa tahun terakhir, kemajuan teknologi informasi telah mendorong transformasi signifikan dalam berbagai aspek kehidupan, termasuk dalam sektor perdagangan. Kemudahan akses internet dan proliferasi perangkat digital telah memfasilitasi pertumbuhan pesat transaksi online di Indonesia. Menurut data dari Kementerian Perdagangan, pengaduan konsumen terkait e-commerce terus meningkat, mencerminkan tingginya aktivitas perdagangan digital di masyarakat (Kementerian Perdagangan, 2022). Seiring dengan meningkatnya transaksi online, kasus penipuan digital juga mengalami lonjakan. Modus operandi yang digunakan pelaku semakin beragam, mulai dari penipuan melalui media sosial hingga situs e-commerce palsu. Fenomena ini menunjukkan bahwa pertumbuhan teknologi tidak selalu diiringi dengan peningkatan kesadaran dan literasi digital masyarakat (Chandra et al., 2025).

Penipuan dalam transaksi digital tidak lagi dilakukan oleh individu semata, melainkan melibatkan jaringan kejahatan terorganisir yang beroperasi lintas negara. Interpol mengungkap bahwa jaringan penipuan dunia maya di Asia Tenggara telah berkembang menjadi jaringan global dengan pendapatan mencapai triliunan dolar AS per tahun. Penegakan hukum terhadap kejahatan digital menghadapi berbagai kendala, termasuk keterbatasan alat dan sumber daya manusia yang kompeten di bidang teknologi informasi. Selain itu, kompleksitas hukum dan kurangnya koordinasi antar lembaga penegak hukum memperparah situasi (Harapansyah et al., 2025).

Meskipun Indonesia telah memiliki regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), implementasinya seringkali tidak efektif. Kesenjangan antara regulasi dan praktik di lapangan menyebabkan banyak kasus penipuan digital tidak tertangani dengan baik (Hafid et al., 2025). (Ruwisanyoto & Sudiarawan, 2025) menekankan bahwa konsumen sebagai pihak yang dirugikan dalam transaksi digital seringkali tidak mendapatkan perlindungan hukum yang memadai. Kurangnya mekanisme pengaduan yang efektif dan lambannya proses hukum membuat pelaku kejahatan merasa tidak jera

Platform digital seperti e-commerce dan media sosial memiliki peran penting dalam mencegah penipuan. Namun, masih banyak platform yang belum memiliki sistem verifikasi dan pengawasan yang ketat terhadap aktivitas pengguna. Peningkatan literasi digital masyarakat menjadi kunci dalam mencegah penipuan online. Edukasi mengenai cara bertransaksi yang aman dan mengenali modus penipuan perlu digalakkan secara masif

Menghadapi kejahatan digital yang bersifat transnasional memerlukan kolaborasi antar

lembaga penegak hukum, baik di dalam negeri maupun internasional. Kerjasama ini penting untuk melacak dan menindak pelaku yang seringkali beroperasi lintas batas negara. Pemanfaatan teknologi canggih seperti kecerdasan buatan dan analitik data dapat membantu penegak hukum dalam mendeteksi dan mencegah kejahatan digital. Investasi dalam teknologi ini menjadi penting untuk meningkatkan efektivitas penegakan hukum. Situasi yang kompleks ini menuntut adanya reformasi hukum dan kebijakan yang adaptif terhadap perkembangan teknologi. Pemerintah perlu merumuskan strategi nasional yang komprehensif untuk menghadapi tantangan kejahatan digital yang semakin kompleks.

Tujuan dari penelitian ini adalah untuk mengidentifikasi dan menganalisis modus serta pola-pola yang digunakan dalam tindak pidana penipuan online, yang semakin berkembang seiring dengan pesatnya penggunaan teknologi digital dalam transaksi. Penelitian ini juga bertujuan untuk menjelaskan secara mendalam elemen-elemen kejahatan terorganisir yang terdapat dalam praktik penipuan tersebut, termasuk struktur jaringan pelaku, pembagian peran, serta strategi yang digunakan untuk mengelabui korban dan aparat penegak hukum. Selain itu, penelitian ini berfokus pada analisis keterkaitan antara kejahatan penipuan online dengan praktik pencucian uang, guna memahami bagaimana hasil dari kejahatan tersebut disamarkan melalui berbagai tahapan finansial, sehingga dapat memberikan kontribusi terhadap upaya pencegahan dan penegakan hukum yang lebih efektif.

METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian yuridis normatif, yaitu penelitian hukum yang dilakukan dengan menelaah bahan pustaka atau data sekunder sebagai dasar untuk meneliti hukum positif, asas hukum, dan doktrin hukum. Metode ini dipilih karena penelitian bertujuan untuk memahami ketentuan hukum yang berlaku mengenai tindak pidana penipuan dalam transaksi online serta keterkaitannya dengan kejahatan terorganisir dan pencucian uang. Namun demikian, pendekatan yuridis empiris juga dapat dilibatkan secara terbatas apabila terdapat data pendukung berupa studi kasus atau hasil wawancara dengan pihak-pihak terkait seperti aparat penegak hukum, korban, atau penyedia jasa keuangan digital.

Pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan (statute approach), yang berfokus pada telaah terhadap peraturan perundang-undangan yang berlaku di Indonesia, terutama Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), Kitab Undang-Undang Hukum Pidana (KUHP), dan Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Pendekatan ini penting untuk melihat bagaimana hukum mengatur serta merespons permasalahan hukum dalam praktik kejahatan siber dan finansial.

Selain itu, digunakan pula pendekatan konseptual (conceptual approach), yang bertujuan untuk mengkaji konsep-konsep dasar yang berkaitan dengan penipuan online, kejahatan terorganisir, dan pencucian uang. Pendekatan ini diperlukan guna memperoleh pemahaman yang lebih mendalam tentang pengertian, elemen-elemen, dan karakteristik dari masing-masing tindak pidana yang diteliti. Dengan menggabungkan kedua pendekatan tersebut, penelitian ini diharapkan mampu memberikan gambaran yang utuh, baik dari sisi normatif maupun konseptual.

Sumber data yang digunakan dalam penelitian ini adalah data sekunder, yang terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer mencakup peraturan perundang-undangan yang relevan, seperti UU ITE, KUHP, dan UU Tindak Pidana Pencucian Uang. Bahan hukum sekunder meliputi buku, jurnal ilmiah, hasil penelitian, dan pendapat para ahli hukum. Sementara itu, bahan hukum tersier berupa ensiklopedia hukum, kamus hukum, serta dokumen lain yang memberikan informasi tambahan terhadap kajian hukum yang dilakukan.

PESHUM : Jurnal Pendidikan, Sosial dan Humaniora
Vol.4, No.3, April 2025

Dalam penelitian ini, apabila tersedia dan relevan, juga akan digunakan data empiris melalui telaah terhadap studi kasus yang pernah terjadi di Indonesia. Kasus-kasus tersebut akan dianalisis untuk melihat implementasi aturan hukum terhadap pelaku penipuan online yang beroperasi secara terorganisir dan diduga melakukan pencucian uang. Studi kasus memberikan kontribusi penting untuk menunjukkan kesenjangan antara teori hukum dengan praktik penegakan hukumnya di lapangan.

Teknik analisis data yang digunakan adalah deskriptif-analitis, yaitu dengan menggambarkan secara sistematis dan menyeluruh mengenai peraturan perundang-undangan dan konsep hukum yang berkaitan dengan pokok bahasan. Penelitian ini tidak hanya memaparkan isi peraturan, tetapi juga menganalisis sejauh mana efektivitas dan kecukupan peraturan tersebut dalam menghadapi tantangan hukum yang ditimbulkan oleh perkembangan teknologi dan modus-modus kejahatan yang semakin kompleks.

Analisis yang dilakukan tidak hanya bersifat teoritis, tetapi juga mencoba mengevaluasi kelemahan regulasi yang ada serta memberikan alternatif pemikiran atau usulan solusi atas permasalahan hukum yang terjadi. Dalam hal ini, penulis juga akan mengaitkan temuan penelitian dengan teori-teori hukum pidana dan hukum siber yang relevan, baik dari literatur nasional maupun internasional.

HASIL DAN PEMBAHASAN

Karakteristik Penipuan dalam Transaksi Online

Perkembangan teknologi informasi telah membawa kemudahan dalam bertransaksi secara online (Dewi & Mahyuni, 2020). Namun, kemajuan ini juga membuka peluang bagi pelaku kejahatan siber untuk melakukan penipuan dalam transaksi online. Penipuan semacam ini menjadi ancaman serius yang dapat merugikan konsumen dan pelaku usaha. Phishing merupakan salah satu modus penipuan yang paling umum dalam transaksi online. Pelaku biasanya mengirimkan email atau pesan palsu yang seolah-olah berasal dari institusi resmi untuk memperoleh informasi sensitif korban, seperti kata sandi atau data kartu kredit. Menurut (Arshad et al., 2021), phishing menjadi ancaman utama di dunia maya karena tekniknya yang terus berkembang dan sulit dideteksi.

Selain phishing, modus scam dan social engineering juga sering digunakan. Scam biasanya melibatkan penawaran palsu atau informasi menyesatkan untuk memancing korban melakukan transaksi. Social engineering memanfaatkan manipulasi psikologis untuk mendapatkan kepercayaan korban. (Sari & Sutabri, 2023) menyoroti bahwa teknik persuasi seperti otoritas dan kelangkaan sering digunakan dalam serangan phishing untuk meningkatkan efektivitasnya. Pelaku penipuan online berasal dari berbagai latar belakang, mulai dari individu hingga sindikat terorganisir. Mereka memanfaatkan anonimitas internet untuk menyembunyikan identitas dan lokasi mereka. Menurut penelitian (Fajariandono et al., 2024), pelaku sering menggunakan teknik social engineering melalui perangkat smartphone untuk menipu korban.

Korban penipuan online tidak terbatas pada kelompok tertentu; siapa pun dapat menjadi target. Namun, penelitian (Adhyaksa & Yudiantara, 2022) menunjukkan bahwa kurangnya kewaspadaan dan pengetahuan tentang modus penipuan membuat konsumen lebih rentan menjadi korban. Kerugian akibat penipuan dalam transaksi online sangat signifikan. Menurut (Bitaab et al., 2021), selama pandemi COVID-19, serangan phishing meningkat drastis, menyebabkan kerugian finansial yang besar bagi individu dan organisasi. Selain kerugian finansial, korban juga mengalami dampak psikologis seperti stres dan kehilangan kepercayaan terhadap transaksi online. Serangan phishing dapat menyebabkan trauma psikologis yang berkepanjangan bagi korban.

Peningkatan edukasi dan kesadaran masyarakat tentang modus penipuan sangat penting. Pentingnya sosialisasi bahaya social engineering untuk meningkatkan kesadaran masyarakat tentang keamanan informasi. Penggunaan teknologi seperti sistem verifikasi dua langkah dan regulasi yang ketat dapat membantu mencegah penipuan. Implementasi teknologi keamanan dalam layanan e-commerce dapat mengurangi risiko serangan phishing. Pemerintah dan lembaga terkait memiliki peran penting dalam menanggulangi penipuan online melalui penegakan hukum dan penyediaan informasi kepada masyarakat. Perlunya kebijakan hukum pidana yang efektif untuk menangani tindak pidana penipuan dalam pembelian barang secara online.

Penipuan dalam transaksi online merupakan masalah kompleks yang memerlukan pendekatan multidisipliner untuk penanggulangannya. Kombinasi antara edukasi, teknologi, regulasi, dan kerjasama antara berbagai pihak dapat membantu mengurangi risiko dan dampak dari penipuan online.

Penipuan Online sebagai Kejahatan Terorganisir

Penipuan online telah berkembang menjadi bentuk kejahatan terorganisir yang kompleks, melibatkan jaringan pelaku dengan pembagian peran yang terstruktur dan pola komunikasi yang canggih. Kejahatan ini tidak lagi dilakukan oleh individu secara mandiri, melainkan oleh kelompok yang terorganisir dengan baik, memanfaatkan teknologi informasi untuk menjalankan aksinya.

Salah satu aspek utama dari penipuan online sebagai kejahatan terorganisir adalah keterlibatan jaringan pelaku yang tersebar di berbagai wilayah. Jaringan ini terdiri dari aktor utama yang merancang dan mengkoordinasikan aksi, serta anggota lain yang menjalankan peran spesifik seperti kurir, pencuci uang, dan perekrut korban. Menurut (Wahyuddin et al., 2024) pelaku utama seringkali menggunakan identitas palsu atau menyamar sebagai institusi resmi untuk memperoleh kepercayaan korban melalui platform seperti WhatsApp Messenger.

Pembagian peran dalam jaringan penipuan online menunjukkan tingkat organisasi yang tinggi. Aktor utama bertanggung jawab atas perencanaan dan pengawasan operasi, sementara kurir bertugas mengirimkan atau menerima barang atau uang hasil penipuan. Pencuci uang memainkan peran penting dalam menyamarkan asal-usul dana ilegal, menjadikannya tampak sah melalui berbagai transaksi keuangan. Selain itu, ada juga perekrut yang mencari korban baru atau anggota tambahan untuk memperluas jaringan.

Pola komunikasi dalam jaringan penipuan online sangat terstruktur dan efisien. Para pelaku menggunakan berbagai platform digital untuk berkomunikasi, seperti aplikasi pesan instan, forum online, dan media sosial. Komunikasi ini seringkali menggunakan kode atau istilah khusus untuk menghindari deteksi oleh pihak berwenang. Menurut penelitian (Nurse & Bada, 2019), kelompok kejahatan siber menggunakan strategi komunikasi yang dirancang untuk menjaga kerahasiaan dan efisiensi operasi mereka.

Modus operandi yang umum digunakan dalam penipuan online meliputi phishing dan sniffing. Phishing melibatkan pengiriman pesan palsu yang tampak berasal dari sumber terpercaya untuk memperoleh informasi pribadi korban. Sniffing, di sisi lain, melibatkan pemantauan lalu lintas data untuk mencuri informasi sensitif. Pelaku sering mengirimkan tautan atau file berbahaya melalui WhatsApp untuk mengelabui korban agar mengunduh malware yang mencuri data pribadi mereka.

Faktor-faktor yang mendorong pertumbuhan penipuan online sebagai kejahatan terorganisir termasuk kemudahan akses ke teknologi, anonimitas yang ditawarkan oleh internet, dan potensi keuntungan finansial yang besar. Selain itu, kurangnya literasi digital di kalangan masyarakat membuat mereka lebih rentan terhadap penipuan. Pentingnya meningkatkan literasi

digital untuk mengurangi risiko menjadi korban penipuan online.

Penegakan hukum terhadap penipuan online menghadapi tantangan signifikan, terutama karena pelaku sering beroperasi lintas negara dan menggunakan teknologi untuk menyembunyikan jejak mereka. Namun, upaya kolaboratif antara lembaga penegak hukum, penyedia layanan internet, dan organisasi internasional dapat meningkatkan efektivitas dalam memberantas kejahatan ini. Menurut (Arigo et al., 2022), pendekatan hukum yang komprehensif diperlukan untuk menangani kompleksitas penipuan online.

Pencegahan penipuan online memerlukan pendekatan multidimensi, termasuk edukasi publik, peningkatan keamanan siber, dan kerjasama internasional. Program edukasi yang menekankan pentingnya menjaga informasi pribadi dan mengenali tanda-tanda penipuan dapat membantu masyarakat menjadi lebih waspada. Selain itu, pengembangan teknologi keamanan yang lebih canggih dapat membantu mendeteksi dan mencegah aktivitas penipuan. Kerjasama internasional juga penting mengingat sifat lintas batas dari penipuan online. Negara-negara perlu berbagi informasi dan sumber daya untuk melacak dan menuntut pelaku yang beroperasi di berbagai yurisdiksi. Inisiatif seperti pertukaran intelijen dan pelatihan bersama dapat meningkatkan kapasitas global dalam memerangi kejahatan siber.

Dalam konteks Indonesia, peningkatan literasi digital dan kesadaran masyarakat terhadap risiko penipuan online menjadi prioritas. Program-program pemerintah dan inisiatif dari sektor swasta yang fokus pada edukasi digital dapat memainkan peran penting dalam mengurangi insiden penipuan. Selain itu, penguatan kerangka hukum dan penegakan hukum yang tegas dapat memberikan efek jera bagi pelaku.

Penipuan online sebagai kejahatan terorganisir merupakan tantangan serius yang memerlukan respons terpadu dari berbagai pihak. Dengan memahami struktur dan modus operandi jaringan penipuan, serta meningkatkan kesadaran dan literasi digital masyarakat, kita dapat mengambil langkah-langkah efektif untuk mencegah dan memberantas kejahatan ini.

Kaitan Penipuan Online dengan Pencucian Uang

Penipuan online dan pencucian uang merupakan dua bentuk kejahatan siber yang saling berkaitan erat. Dalam banyak kasus, hasil dari penipuan online digunakan sebagai dana awal dalam proses pencucian uang. Pelaku kejahatan siber seringkali memanfaatkan celah dalam sistem keuangan digital untuk menyembunyikan asal-usul dana ilegal tersebut (Pratama, 2025). Dengan berkembangnya teknologi finansial, modus operandi pencucian uang menjadi semakin kompleks dan sulit dideteksi.

Proses pencucian uang umumnya terdiri dari tiga tahap utama: placement, layering, dan integration. Tahap pertama, placement, melibatkan penempatan dana ilegal ke dalam sistem keuangan formal, seperti melalui setoran tunai ke rekening bank atau pembelian instrumen keuangan. Tahap kedua, layering, bertujuan untuk memisahkan dana dari sumber ilegalnya melalui serangkaian transaksi kompleks, seperti transfer antar rekening atau pembelian aset digital. Tahap terakhir, integration, adalah proses menggabungkan dana yang telah "dibersihkan" ke dalam ekonomi legal, misalnya melalui investasi atau pembelian properti .

Dalam konteks penipuan online, alur dana hasil kejahatan seringkali mengikuti pola yang serupa. Setelah berhasil menipu korban, pelaku segera memindahkan dana ke rekening lain atau mengonversinya ke bentuk aset digital untuk menghindari deteksi. Proses ini memanfaatkan berbagai instrumen keuangan digital yang menawarkan anonimitas dan kemudahan transaksi lintas batas. Dengan demikian, pelaku dapat dengan cepat menyamarkan jejak dana dan mengintegrasikannya ke dalam sistem keuangan legal.

Salah satu instrumen yang sering digunakan dalam pencucian uang adalah rekening palsu. Pelaku kejahatan siber seringkali membuka rekening bank dengan identitas fiktif atau

menggunakan identitas orang lain tanpa izin. Rekening ini kemudian digunakan untuk menampung dana hasil kejahatan sebelum dipindahkan ke rekening lain atau dikonversi ke bentuk aset digital. Penggunaan rekening palsu mempersulit pihak berwenang dalam melacak aliran dana dan mengidentifikasi pelaku sebenarnya.

Selain rekening palsu, e-wallet atau dompet digital juga menjadi sarana favorit bagi pelaku pencucian uang. Layanan e-wallet menawarkan kemudahan dalam melakukan transaksi tanpa harus melalui proses verifikasi yang ketat. Beberapa e-wallet bahkan memungkinkan pengguna untuk melakukan transaksi anonim, sehingga sulit bagi pihak berwenang untuk melacak aliran dana. Dengan memanfaatkan e-wallet, pelaku dapat dengan mudah memindahkan dana antar akun atau mengonversinya ke bentuk lain tanpa terdeteksi.

Cryptocurrency, seperti Bitcoin, juga sering digunakan dalam proses pencucian uang. Karakteristik cryptocurrency yang menawarkan anonimitas, desentralisasi, dan kemudahan transaksi lintas batas menjadikannya alat yang ideal bagi pelaku kejahatan siber (Puanandini, 2021). Pelaku dapat dengan mudah mengonversi dana hasil kejahatan ke dalam bentuk cryptocurrency, memindahkannya ke berbagai dompet digital, dan akhirnya mengonversinya kembali ke mata uang fiat tanpa meninggalkan jejak yang jelas .

Namun, penggunaan cryptocurrency dalam pencucian uang juga menghadirkan tantangan baru bagi pihak berwenang. Kurangnya regulasi yang jelas dan keterbatasan dalam teknologi pelacakan membuat proses penegakan hukum menjadi lebih sulit. Selain itu, sifat desentralisasi dari cryptocurrency berarti tidak ada otoritas pusat yang dapat dimintai pertanggungjawaban atau diminta untuk memberikan informasi transaksi. Hal ini memperumit upaya untuk melacak dan membekukan aset yang terlibat dalam pencucian uang.

Untuk mengatasi tantangan ini, beberapa negara telah mulai mengimplementasikan regulasi yang lebih ketat terhadap penggunaan cryptocurrency. Misalnya, beberapa negara mewajibkan platform pertukaran cryptocurrency untuk menerapkan prosedur Know Your Customer (KYC) dan Anti-Money Laundering (AML). Dengan langkah ini, diharapkan dapat meningkatkan transparansi dan memudahkan pihak berwenang dalam melacak aliran dana yang mencurigakan.

Di Indonesia, upaya untuk mencegah dan memberantas pencucian uang juga terus dilakukan. Pemerintah telah mengeluarkan berbagai regulasi yang mengatur tentang transaksi keuangan digital dan mewajibkan penyedia layanan keuangan untuk melaporkan transaksi mencurigakan. Selain itu, edukasi kepada masyarakat tentang bahaya penipuan online dan pentingnya menjaga keamanan data pribadi juga menjadi fokus utama dalam upaya pencegahan.

Namun, tantangan tetap ada, terutama dalam hal penegakan hukum dan koordinasi antar lembaga. Kurangnya sumber daya dan teknologi yang memadai seringkali menjadi hambatan dalam mengidentifikasi dan menindak pelaku pencucian uang. Oleh karena itu, diperlukan kerjasama yang lebih erat antara pemerintah, sektor swasta, dan masyarakat untuk menciptakan ekosistem keuangan digital yang aman dan bebas dari kejahatan.

Penipuan online dan pencucian uang merupakan ancaman serius bagi stabilitas sistem keuangan dan keamanan masyarakat. Dengan memahami modus operandi dan instrumen yang digunakan oleh pelaku, serta memperkuat regulasi dan penegakan hukum, diharapkan dapat mengurangi risiko dan dampak dari kejahatan ini. Peningkatan literasi digital dan kesadaran masyarakat juga menjadi kunci dalam menciptakan lingkungan digital yang aman dan terpercaya.

Analisis Yuridis

Analisis yuridis terhadap penipuan online dan pencucian uang di Indonesia memerlukan kajian mendalam terhadap regulasi yang berlaku, termasuk Kitab Undang-Undang Hukum Pidana

(KUHP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Penegakan hukum terhadap kejahatan siber ini menghadapi berbagai tantangan, baik dari segi substansi hukum maupun implementasinya di lapangan.

Dalam KUHP, penipuan diatur dalam Pasal 378 yang menyatakan bahwa barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, atau rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang, memberikan utang, atau menghapuskan piutang, diancam dengan pidana penjara paling lama empat tahun. Namun, ketentuan ini belum secara spesifik mengatur penipuan yang dilakukan melalui media elektronik.

UU ITE hadir untuk mengisi kekosongan hukum tersebut. Pasal 28 ayat (1) UU ITE mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik dapat dikenai sanksi pidana. Pasal ini memberikan landasan hukum bagi penegakan terhadap penipuan yang dilakukan melalui media elektronik, termasuk penipuan online.

Namun, dalam praktiknya, terjadi tumpang tindih antara KUHP dan UU ITE dalam mengatur penipuan. Prinsip lex specialis derogat legi generali menyatakan bahwa hukum yang bersifat khusus mengesampingkan hukum yang bersifat umum. Oleh karena itu, dalam kasus penipuan online, UU ITE sebagai lex specialis seharusnya lebih diutamakan dalam penegakan hukum. Hal ini ditegaskan dalam penelitian oleh (Nurrazaq & Setyorini, 2024) yang menyatakan bahwa UU ITE memberikan kerangka hukum yang lebih spesifik untuk menangani penipuan dalam transaksi elektronik.

Selain penipuan, pencucian uang juga menjadi perhatian serius dalam konteks kejahatan siber. UU Nomor 8 Tahun 2010 mengatur tentang pencegahan dan pemberantasan tindak pidana pencucian uang. Undang-undang ini memberikan kewenangan kepada aparat penegak hukum untuk menyita dan merampas aset yang diduga berasal dari tindak pidana, termasuk hasil penipuan online. Pentingnya penerapan UU ini dalam menangani pencucian uang yang dilakukan melalui investasi ilegal.

Namun, penegakan hukum terhadap pencucian uang menghadapi berbagai tantangan. Salah satunya adalah kesulitan dalam melacak aliran dana yang telah melalui berbagai lapisan transaksi untuk menyamarkan asal-usulnya. Selain itu, penggunaan teknologi canggih oleh pelaku kejahatan siber menyulitkan aparat dalam mengidentifikasi dan membuktikan tindak pidana pencucian uang. Penelitian oleh (Cahyono & Hidayati, 2020) menekankan perlunya peningkatan kapasitas aparat penegak hukum dalam menghadapi tantangan ini.

Kelemahan lain dalam penegakan hukum adalah kurangnya koordinasi antara lembaga penegak hukum dan lembaga keuangan. Kerjasama yang efektif antara kepolisian, kejaksaan, pengadilan, dan lembaga keuangan sangat penting untuk mendeteksi dan mencegah pencucian uang. Sinergi antar lembaga dapat meningkatkan efektivitas penegakan hukum terhadap tindak pidana pencucian uang.

Selain itu, tantangan juga muncul dalam hal pembuktian di pengadilan. Dalam kasus penipuan online dan pencucian uang, pembuktian seringkali bergantung pada bukti digital yang mudah dimanipulasi atau dihapus. Oleh karena itu, diperlukan perangkat hukum dan teknologi yang memadai untuk mengumpulkan dan memverifikasi bukti digital Pentingnya penguatan kapasitas aparat dalam menangani bukti digital.

Di sisi lain, perlindungan terhadap korban penipuan online juga perlu mendapat perhatian. Korban seringkali mengalami kerugian finansial yang signifikan dan kesulitan dalam

mendapatkan ganti rugi. Oleh karena itu, sistem hukum perlu memberikan mekanisme yang efektif untuk pemulihan kerugian korban. Pentingnya pendekatan victimologi dalam penanganan kasus penipuan online.

Untuk mengatasi berbagai kelemahan dan tantangan tersebut, diperlukan reformasi hukum yang komprehensif. Reformasi ini meliputi pembaruan regulasi yang relevan, peningkatan kapasitas aparat penegak hukum, serta penguatan kerjasama antar lembaga. Selain itu, edukasi kepada masyarakat tentang bahaya penipuan online dan pentingnya kewaspadaan dalam transaksi elektronik juga sangat penting.

Penegakan hukum terhadap penipuan online dan pencucian uang memerlukan pendekatan yang holistik dan terintegrasi. Dengan memperkuat kerangka hukum, meningkatkan kapasitas aparat, dan melibatkan berbagai pemangku kepentingan, diharapkan dapat tercipta sistem hukum yang efektif dalam menghadapi kejahatan siber di era digital ini.

KESIMPULAN

Penelitian ini menemukan bahwa penipuan online tidak lagi berdiri sebagai tindak pidana tunggal, melainkan telah menjadi bagian dari skema kejahatan terorganisir yang terstruktur dan kompleks. Para pelaku seringkali bekerja dalam jaringan dengan peran dan tugas yang terdistribusi, seperti pengelola akun palsu, perekrut korban, hingga pihak yang bertanggung jawab dalam memindahkan dana hasil kejahatan. Modus operandi yang digunakan semakin canggih dan memanfaatkan celah dalam sistem digital, sehingga menyulitkan identifikasi dan pelacakan. Hasil dari penipuan ini umumnya disamarkan melalui praktik pencucian uang, dengan menggunakan rekening pihak ketiga, aset digital, atau transaksi antarnegara untuk mengaburkan asal-usul dana. Keterkaitan erat antara ketiga elemen ini menunjukkan perlunya penanganan hukum yang komprehensif dan lintas sektor untuk memutus rantai kejahatan tersebut.

Untuk menghadapi dinamika kejahatan digital yang terus berkembang, diperlukan regulasi yang lebih adaptif dan responsif terhadap bentuk-bentuk kejahatan siber yang bersifat lintas negara, serta mekanisme hukum yang mampu menjawab tantangan teknologi informasi. Penegakan hukum juga perlu diperkuat, baik dari sisi substansi hukum maupun kapasitas sumber daya manusia. Aparat penegak hukum perlu dibekali dengan pengetahuan dan keterampilan khusus dalam menangani kejahatan yang melibatkan teknologi tinggi dan jaringan internasional. Selain itu, edukasi publik secara masif juga menjadi bagian penting dalam strategi pencegahan. Masyarakat perlu diberi pemahaman mengenai bahaya dan modus penipuan online, serta cara-cara aman bertransaksi digital agar tidak menjadi korban kejahatan. Dengan sinergi antara regulasi, penegakan hukum, dan kesadaran masyarakat, diharapkan dapat tercipta ekosistem digital yang lebih aman dan terlindungi dari kejahatan terorganisir.

DAFTAR REFERENSI

Adhyaksa, S. G., & Yudiantara, I. G. N. N. K. (2022). Peranan Korban Dalam Terjadinya Tindak Pidana Penipuan Dalam Belanja Online. *Kertha Semaya: Journal Ilmu Hukum*, *10*(8), 1779.

Arigo, M., Tambunan, M., & Siregar, G. (2022). Akibat Hukum Bagi Pelaku Tindak Pidana Penipuan Online Melalui Modus Arisan Online Di Media Sosial Elektronik. *Jurnal Rectum: Tinjauan Yuridis Penanganan Tindak Pidana, 4*(2), 182-190. http://dx.doi.org/10.46930/jurnalrectum.v4i2.1733

Arshad, A., Rehman, A. U., Javaid, S., Ali, T. M., Sheikh, J. A., & Azeem, M. (2021). A

Systematic Literature Review On Phishing And Anti-Phishing Techniques. *arXiv preprint arXiv:2104.01255*.

Astiti, N. M. Y. A. (2024). Pengaturan Tindak Pidana Penipuan Secara Elektronik Dalam Hukum Positif Indonesia. *Widyasrama*, *37*(2), 1-12.

Bastari, R. G., Junaidi, A., & Ismiyanto, I. (2024). Perlindungan Hukum Terhadap Tindak Pidana Penipuan dalam Situs Jual Beli Online di Indonesia. *Ranah Research: Journal of Multidisciplinary Research and Development*, *7*(1), 287-294. https://doi.org/10.38035/rrj.v7i1.1226

Bitaab, M., Cho, H., Oest, A. Zhang, P., Sun, Z., Pourmohamad, R., Kim, D., Bao, T., Wang, R., Shoshitaishvili, Y., Doupe´A. & Ahn, G. (2020). Scam Pandemic: How Attackers Exploit Public Fear through Phishing. *APWG Symposium on Electronic Crime Research (eCrime).*

Cahyono, J., & Hidayati, A. (2020). Peranan Kepolisian dalam Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. *Jurnal Ilmiah Hukum: Inrichting Recht*, *2*(2).

Chandra, T., Munawar, A., & Aini, M. . (2025). Tinjauan Yuridis terhadap Mekanisme Penyelidikan pada Tindak Pidana Penipuan Melalui Media Transaksi Elektronik oleh Kepolisian dalam Sistem Peradilan Pidana di Indonesia. *Jurnal Hukum Lex Generalis*, *5*(7).

Dewi, N. K. A., & Mahyuni, L. P. (2020). Pemetaan Bentuk Dan Pencegahan Penipuan E-Commerce. *E-Jurnal Ekonomi Dan Bisnis Universitas Udayana,* , 851-878. https://doi.org/10.24843/EEB.2020.v09.i09.p03

Fajariandono, D., Sitorus, W. W., Desianto, E., Aer, F., Rahim, A., & Pramata, Y. A. (2024). Upaya Risk Management Dalam Mengatasi Penipuan Modus Social Engineering Melalui Smartphone. *EKOMA: Jurnal Ekonomi, Manajemen, Akuntansi*, *3*(3), 752-759.

Hafid, N. S., Rusmana, D., & Shaleh, C. (2025). Penerapan Teori Pidana dalam Pencegahan dan Penanggulangan Kriminalitas: Studi Kasus dan Tantangan Implementasi. *Legalite: Jurnal Perundang Undangan dan Hukum Pidana Islam*, *10*(1), 85-104.

Harapansyah, M., Rahman, S., & Badaru, B. (2025). The Effectiveness of Law Enforcement for Criminal Fraud via WhatsApp in the Legal Area of the Pasangkayu Police. *International Journal on Advanced Science, Education, and Religion*, *8*(1), 77-93.

Hisyam, C. J., Fadila, E. N., Novia, E., Syawaldi, F. P., Regitha, N., & Febriyani, R. (2024). Analisis Kejahatan Korupsi Ditinjau Dari Kejahatan Terorganisir. *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora*, *2*(1), 15-24. DOI: https://doi.org/10.59246/aladalah.v2i1.610

Kementerian Perdagangan. (2022). Kemendag catat pengaduan konsumen 2021, e-commerce kembali mendominasi. Diakses melalui https://www.kemendag.go.id/id/pers/kemendag-catat-pengaduan-konsumen2021-e-commerce-kembali-mendominasi-1 pada 12 Maret 2025.

Mardiyati, S. (2022). Strategi Pencegahan Dan Pemberantasan Pencucian Uang Dan Tahapan-Tahapan Tindak Pidana Pencucian Uang. *Disiplin: Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda*, *28*(4), 215-220.

Nurrazaq, M., & Setyorini, E. H. (2024). Pengaturan Tindak Pidana Penipuan Secara Online

Dengan Modus Kerja Paruh Waktu. *Jurnal Literasi Indonesia*, *1*(3), 83-89.

Nurse, J. R. C., & Bada, M. (2019). The group element of cybercrime: Types, dynamics, and criminal operations. In A. Attrill-Smith, C. Fullwood, M. Keep, & D. J. Kuss (Eds.), *The Oxford handbook of cyberpsychology* (pp. 691–715). Oxford University Press.

Pratama, A. (2025). Peran Keuangan Digital Dalam Mendeteksi Dan Mencegah Tindak Pidana Pencucian Uang Pada Transaksi Elektronik. *Sumbang12 Law Journal*, *3*(2), 250-260.

Puanandini, D. A. (2021). Pidana Pencucian Uang Hasil Kejahatan Siber (Cyber Crime) Melalui Mata Uang Digital (Crypto Currency). *Pemuliaan Hukum*, *4*(2), 57-70.

Purba, N., Muhlizar, S. W., & Siregar, F. N. (2023). Tindak Pidana Penipuan Bisnis Online Di Tinjau Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Ite. Jurnal Penelitian Pendidikan Sosial Humaniora, 8(1), 109-114. https://doi.org/10.32696/jp2sh.v8i1.2082

Ruwisanyoto, R. F. A. P., & Sudiarawan, K. A. (2025). Perlindungan Hukum terhadap Konsumen dalam Kecurangan dan Penipuan Transaksi E-Commerce. *Ethics and Law Journal: Business and Notary*.

Sari, P., & Sutabri, T. (2023). Analisis Kejahatan Online Phising Pada Institusi Pemerintah/Pendidik Sehari-Hari. *Jurnal Digital Teknologi Informasi*, *6*(1), 29-34.

Sari, V. K., & Nasution, M. I. P. (2024). Dampak E-commerce Terhadap Perkembangan Digital. *Jurnal Akademik Ekonomi Dan Manajemen*, *1*(4), 18-24.

Siegel, D. (2020). Illegal Mining: Organized Crime, Corruption, Ecocide in a Resource-Scare World (First). Palgrave Macmillan.

Simbolon, M. M., Kesuma, I. G. K. W., & Wibowo, A. E. (2021). Kejahatan Siber pada Penyelenggaraan Perdagangan Berbasis Sistem Elektronik Dalam langkah Pengamanan Pertumbuhan Ekonomi Digital Indonesia. *Defendonesia*, *5*(1), 1-12.

Wahyuddin, Ersa, L. F., Aningsih, G., Hidayat, T., & Sonni, A. F. (2024). Analisis jaringan komunikasi penipuan online melalui media sosial WhatsApp Messenger. *Jurnal Netnografi Komunikasi*, *2*(2), 73-90.