Parlementer : Jurnal Studi Hukum dan Administrasi Publik
Volume. 2 Nomor. 4 Desember 2025
e-ISSN : 3063-122X; p-ISSN : 3063-1238, Hal. 92-105
DOI: https://doi.org/10.62383/parlementer.v2i4.1425
Tersedia: https://ejournal.appihi.or.id/index.php/Parlementer

Penipuan *Online* sebagai Bentuk Kejahatan Siber dalam Perspektif Kriminologi

Anisa Sahara[1*], Kuswandi[2]
[1-2]Ilmu Hukum, Universitas Suryakancana, Indonesia
Email: anisaasahara@gmail.com[1], kuswandi@unsur.ac.id[2]*

**Penulis Korespondensi: anisaasahara@gmail.com*

Abstract. *This study analyzes online fraud as one of the most common forms of cybercrime in Indonesia, which has expanded alongside rapid advances in information and communication technology. These crimes utilize digital platforms such as social media, online marketplaces, and fraudulent websites to deceive victims for unlawful financial gain. The research aims to examine online fraud from a criminological perspective by identifying its causes, patterns, and relevance to routine activity theory and differential association theory. A normative juridical method is employed, using statutory, conceptual, and case-based approaches, with qualitative and descriptive analysis. The findings show that online fraud reflects a shift from conventional fraud to digital-based crimes, driven by low public awareness of cybersecurity, easy access to technology, and weak online supervision. Several fraud schemes were identified, including online investment scams, phishing, and identity impersonation. This study highlights the need for an integrated approach that goes beyond law enforcement by emphasizing digital literacy, public education, and cross-sector collaboration to reduce cybercrime in Indonesia.*

Keywords: *Criminology; Cybercrime; Information Technology; Law Enforcement; Online Fraud.*

Abstrak. Penelitian ini mengkaji penipuan *online* sebagai salah satu bentuk kejahatan siber yang paling banyak terjadi di Indonesia, seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi. Tindak pidana ini memanfaatkan berbagai platform digital, seperti media sosial, pasar daring, dan situs web palsu, untuk menipu korban demi memperoleh keuntungan finansial secara melawan hukum. Penelitian ini bertujuan menganalisis penipuan daring dari perspektif kriminologi dengan mengkaji faktor penyebab, pola kejahatan, serta keterkaitannya dengan teori aktivitas rutin dan teori *differential association*. Metode yang digunakan adalah pendekatan yuridis normatif melalui pendekatan peraturan perundang-undangan, konseptual, dan studi kasus, dengan analisis kualitatif deskriptif. Hasil penelitian menunjukkan bahwa penipuan daring merupakan pergeseran dari penipuan konvensional ke bentuk kejahatan berbasis digital, yang dipengaruhi oleh rendahnya kesadaran masyarakat terhadap keamanan siber, kemudahan akses teknologi, serta lemahnya pengawasan di ruang digital. Bentuk penipuan yang ditemukan antara lain penipuan investasi online, *phishing*, dan penyamaran identitas. Penelitian ini menegaskan pentingnya pendekatan terpadu yang tidak hanya berfokus pada penegakan hukum, tetapi juga pada peningkatan literasi digital, edukasi publik, dan kerja sama lintas sektor untuk menekan angka kejahatan siber di Indonesia.

Kata kunci: Kejahatan Siber; Kriminologi; Penegakan Hukum; Penipuan Online; Teknologi Informasi.

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah memberikan dampak besar terhadap perubahan cara masyarakat menjalankan hubungan sosial serta kegiatan ekonomi. Pemanfaatan internet dalam bidang perdagangan, layanan perbankan, dan penyelenggaraan pelayanan publik memang meningkatkan efisiensi, namun pada saat yang sama juga menciptakan ruang baru bagi munculnya kejahatan siber. Salah satu bentuk kejahatan siber yang paling sering terjadi dan menimbulkan keresahan di kalangan masyarakat Indonesia adalah penipuan *online*. Praktik penipuan tersebut umumnya dilakukan dengan memanfaatkan media sosial, platform *marketplace*, aplikasi pesan instan, serta *website* palsu. Kondisi ini

Naskah Masuk: 28 Oktober 2025; Revisi: 30 November 2025; Diterima: 20 Desember 2025; Terbit: 31 Desember 2025

menunjukkan bahwa tindak kejahatan tidak lagi terbatas pada ranah fisik, melainkan telah berkembang dan berlangsung secara luas di ruang digital.

Penipuan *online* merupakan bentuk tindak pidana yang memanfaatkan teknologi digital dan jaringan internet untuk menipu korban dengan tujuan memperoleh keuntungan secara melawan hukum. Jenis kejahatan ini memiliki ciri yang berbeda dari kejahatan biasa karena dilakukan tanpa berhadapan muka, bisa terjadi di berbagai wilayah bahkan lintas negara, serta sering kali sulit ditelusuri karena pelakunya beroperasi secara anonymous di dunia maya. Kondisi ini membuat penipuan *online* berkembang sangat cepat dan menjadi ancaman besar bagi keamanan masyarakat di dunia digital. Penipuan *online* yang dilakukan melalui metode *social engineering* kerap dimanfaatkan dalam kejahatan di sektor perbankan, di mana pelaku menyamar sebagai petugas bank untuk mendapatkan data pribadi milik korban, seperti kode OTP (*One-Time Password*) dan informasi sensitif lainnya (Nur, 2025).

Secara hukum, tindakan penipuan *online* dapat diancam dengan Pasal 378 KUHP yang mengatur tindak pidana penipuan. Selain itu, juga terdapat ketentuan khusus dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016, khususnya Pasal 28 ayat (1) dan Pasal 45A ayat (1). Namun demikian, angka kasus penipuan *online* yang tinggi menunjukkan bahwa pendekatan hukum pidana sendiri belum cukup berhasil dalam mengurangi maraknya tindak kejahatan ini (Wahyudi et al., 2022).

Penipuan klasik umumnya dilakukan dengan cara bertemu langsung, seperti memberi informasi palsu secara lisan atau menggunakan dokumen yang tidak asli. Namun, pada penipuan *online*, pelaku menggunakan akun media sosial palsu, situs web yang menyerupai aslinya, aplikasi pesan instan, hingga teknik *phishing* untuk menipu korban. Perkembangan ini menunjukkan bahwa penipuan *online* sebenarnya adalah bentuk pergeseran dari penipuan konvensional ke bentuk digital, bukan jenis kejahatan baru (Amelia, 2023). Karena itu, pemahaman tentang penipuan klasik tetap penting untuk memahami penipuan *online*. Penipuan *online* merupakan perbuatan melawan hukum yang dilakukan dengan memanfaatkan jaringan internet maupun aplikasi berbasis internet sebagai sarana untuk memperdaya pihak lain atau memperoleh keuntungan secara tidak sah (Butarbutar, 2023). Praktik penipuan *online* kerap dilakukan melalui penggunaan identitas atau foto palsu, serta penyampaian informasi yang tidak sesuai dengan kenyataan guna memperoleh keuntungan dari pihak lain. Aktivitas tersebut dapat berlangsung melalui berbagai *platform* media sosial maupun sarana elektronik lainnya, yang pada akhirnya dapat menyebabkan kerugian bagi pihak korban, baik dalam bentuk

kerugian ekonomi maupun dampak terhadap kondisi fisik atau jasmaninya (Mulyadi et al., 2024).

Dalam praktiknya, angka penipuan *online* yang tinggi menunjukkan bahwa cara hukum yang hanya menindak pelaku belum cukup berhasil mengurangi kejahatan ini. Laporan dari Kepolisian Negara Republik Indonesia, Kementerian Komunikasi dan Informatika, serta Otoritas Jasa Keuangan menunjukkan bahwa penipuan *online* adalah jenis kejahatan siber dengan laporan tertinggi dalam beberapa tahun terakhir. Kondisi ini menunjukkan bahwa faktor-faktor sosial, ekonomi, dan budaya juga berperan dalam meningkatkan terjadinya penipuan *online*.

Oleh karena itu, studi kriminologi sangat penting untuk memahami tindak pencurian *online* tidak hanya sebagai tindakan melanggar hukum, tetapi juga sebagai fenomena sosial yang dipengaruhi oleh berbagai faktor, seperti kondisi individu, lingkungan sekitar, serta struktur masyarakat. Penelitian ini bertujuan untuk menganalisis pencurian *online* sebagai bentuk kejahatan siber dari sudut pandang kriminologi, dengan mengeksplorasi penyebabnya, pola pelakuan kejahatan, serta hubungannya dengan berbagai teori kriminologi. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam bentuk konsep dan rekomendasi untuk upaya mencegah serta mengatasi kejahatan siber di Indonesia.

2. KAJIAN TEORITIS

Penipuan *online* merupakan perbuatan dengan sengaja menipu orang lain melalui sarana elektronik untuk memperoleh keuntungan secara melawan hukum. Unsur-unsur penipuan sebagaimana diatur dalam Pasal 378 KUHP, yang mencakup penggunaan berbagai bentuk tipu daya, penyusunan kebohongan secara berulang, serta adanya niat untuk memperoleh keuntungan bagi diri sendiri ataupun pihak lain dengan cara yang bertentangan dengan hukum, meskipun dilakukan dalam lingkungan digital (Lubis et al., 2023). Perbedaannya terletak pada media dan modus operandi yang memanfaatkan teknologi informasi. Tindak pidana siber adalah tindakan kriminal yang berkaitan dengan dunia maya atau menggunakan komputer. Jika seseorang menggunakan komputer atau bagian dari jaringan komputer secara melanggar undang-undang, tindakan tersebut dapat dikategorikan sebagai tindak pidana siber (Ratulangi et al., 2021). Berdasarkan ketentuan dalam UU ITE, struktur kejahatan siber dapat diklasifikasikan ke dalam dua kelompok utama. Kelompok pertama mencakup kejahatan yang secara langsung menyasar internet, sistem komputer, serta teknologi yang berkaitan dengannya. Dalam UU ITE, terdapat tujuh jenis tindak pidana yang digolongkan sebagai kejahatan yang menargetkan internet, komputer, dan teknologi terkait. Jenis-jenis kejahatan ini

dipandang sebagai bentuk kejahatan yang bersifat dinamis dan terus berkembang, sehingga berpotensi melahirkan varian kejahatan baru (Rantesalu, 2022).

Teori *Routine Activity*

Cohen dan Felson melalui teori aktivitas rutin menjelaskan bahwa seseorang dapat menjadi korban kejahatan bukan semata-mata karena faktor pelaku, melainkan juga akibat ekspektasi tidak langsung yang terbentuk dari aktivitas keseharian. Teori ini berangkat dari asumsi bahwa aktivitas yang dilakukan secara berulang dan konsisten dalam kehidupan sehari-hari akan membentuk pola tertentu. Pola aktivitas tersebut pada akhirnya dapat meningkatkan tingkat kerentanan individu, baik dari segi kondisi maupun situasi yang dihadapi. Lebih lanjut, teori aktivitas rutin menegaskan bahwa terjadinya kejahatan dan timbulnya korban dipengaruhi oleh keberadaan tiga unsur utama. Pertama, adanya target yang sesuai, yaitu individu atau objek yang menjadi sasaran kejahatan karena memiliki tingkat kerentanan tertentu dalam aktivitas rutinnya. Aktivitas yang dilakukan secara berulang dengan pola yang mudah diprediksi berpotensi meningkatkan risiko viktimisasi. Kedua, keberadaan penjagaan yang memadai, yakni bentuk pengawasan atau perlindungan yang efektif, seperti kontrol sosial dari lingkungan sekitar, pengawasan orang tua, maupun pemanfaatan teknologi keamanan. Ketiga, keberadaan pelaku yang memiliki motivasi, yaitu individu atau kelompok yang tidak hanya mempunyai kapasitas untuk melakukan kejahatan, tetapi juga memiliki niat serta perencanaan untuk merealisasikannya (Waskito & Nurhadiyanto, 2020).

Teori *Differential Association*

Teori kriminologi bisa digunakan untuk menganalisis berbagai masalah yang berkaitan dengan kejahatan atau penyebab terjadinya kejahatan, termasuk tindak pidana terorisme. Secara dasar, teori-teori kriminologi bertujuan untuk meneliti dan menjelaskan berbagai hal yang terkait dengan perilaku penjahat dan tindakan criminal (Situmeang, 2021). Teori *Differential Association* yang dikemukakan oleh Edwin H. Sutherland menegaskan bahwa perilaku kriminal tidak bersumber dari faktor biologis atau diwariskan secara genetis dari orang tua kepada anak. Sebaliknya, kecenderungan untuk melakukan kejahatan terbentuk melalui proses pembelajaran sosial yang berlangsung dalam lingkungan pergaulan yang bersifat dekat dan intens. Dalam konteks ini, perilaku menyimpang dipelajari melalui interaksi dan komunikasi antar anggota kelompok, di mana individu tidak hanya memperoleh pengetahuan mengenai teknik atau cara melakukan kejahatan, tetapi juga mempelajari nilai, motif, serta pembenaran yang digunakan untuk mendukung tindakan kriminal. Oleh karena itu, kajian mengenai pelaku tindak pidana terorisme dapat dianalisis dengan menggunakan perspektif

kriminologi sosial, yang menekankan peran lingkungan sosial dan proses pembelajaran dalam membentuk perilaku kejahatan.

3. METODE PENELITIAN.

Penelitian ini menerapkan metode yuridis normatif dengan menggunakan pendekatan peraturan perundang-undangan, pendekatan konseptual, dan pendekatan berbasis kasus. Bahan hukum primer yang dijadikan rujukan meliputi Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta berbagai ketentuan peraturan perundang-undangan lain yang relevan. Adapun bahan hukum sekunder terdiri atas artikel jurnal ilmiah, literatur kriminologi, serta laporan resmi yang diterbitkan oleh Kepolisian Negara Republik Indonesia, Kementerian Komunikasi dan Informatika, dan Otoritas Jasa Keuangan. Selain itu, bahan hukum tersier mencakup kamus hukum dan ensiklopedia hukum. Proses analisis data dilakukan secara kualitatif dengan menggunakan teknik deskriptif-analitis.

4. HASIL DAN PEMBAHASAN

Berdasarkan data statistik mengenai kejahatan siber yang diterbitkan melalui situs resmi pengaduan kejahatan siber nasional, terlihat bahwa penipuan *online* adalah jenis kejahatan yang paling banyak dilaporkan oleh masyarakat. Jumlah laporan terkait penipuan *online* tercatat mencapai 14.496 kasus, yang menunjukkan tingginya intensitas kejahatan tersebut di tengah masyarakat. Berbagai modus operandi digunakan oleh pelaku dalam melakukan penipuan, antara lain penipuan investasi, penipuan berkedok undian atau hadiah, penipuan di bidang pekerjaan dan ketenagakerjaan, penipuan dengan dalih layanan dukungan teknis, penipuan berbasis hubungan personal atau romansa, penipuan kartu kredit, hingga penipuan dalam transaksi belanja online. Keberagaman modus tersebut menggambarkan kompleksitas dan dinamika penipuan online yang terus berkembang seiring dengan pemanfaatan teknologi digital. Angka yang tinggi ini menunjukkan bahwa perkembangan transaksi dan interaksi digital sudah dimanfaatkan secara luas oleh pelaku kejahatan untuk mendapatkan keuntungan secara tidak sah (Patroli Siber, 2025).

Gambaran Umum Penipuan *Online* di Indonesia

Media *online* merupakan berbagai bentuk media yang dapat diakses melalui jaringan internet, mencakup penyajian informasi dalam bentuk teks, gambar, audio, maupun video. Media ini juga dapat dipahami sebagai sarana komunikasi yang berlangsung secara digital melalui *email*, *website*, aplikasi pesan instan seperti *WhatsApp*, serta platform media sosial

antara lain *Facebook*, *Instagram*, *Twitter*, dan sejenisnya. Media *online* kerap disebut sebagai *digital media*. Keberadaan media *online* memiliki peranan yang signifikan dalam memfasilitasi interaksi dan komunikasi antarpengguna. (Kustiawan et al., 2022). Sebagai sarana berbasis digital, media daring menyediakan ruang yang luas bagi penggunanya untuk menjalin interaksi sosial, melakukan komunikasi, serta mendistribusikan berbagai bentuk konten tanpa dibatasi oleh ruang dan waktu. Kehadiran media *online* memberikan dampak signifikan terhadap kehidupan sosial masyarakat, khususnya dalam membentuk perubahan pada pola perilaku, cara berpikir, dan gaya hidup. Melalui media daring, masyarakat memiliki kesempatan untuk berinteraksi secara lebih terbuka dan memperoleh informasi dari berbagai sumber, sehingga media berperan sebagai fasilitator bagi individu untuk mengakses informasi serta mengekspresikan diri secara bebas. Di sisi lain, perkembangan media sosial turut memengaruhi munculnya berbagai bentuk penipuan di tengah masyarakat. Pesatnya kemajuan teknologi digital menyebabkan akses terhadap layanan dan informasi *online* menjadi semakin mudah. Namun, rendahnya tingkat literasi dan kewaspadaan masyarakat dalam menggunakan media sosial menjadikan mereka lebih rentan terhadap kejahatan siber. Salah satu bentuk kejahatan yang kerap terjadi adalah penipuan berbasis *online*, yang umumnya dilakukan melalui penyampaian pesan-pesan persuasif yang dirancang sedemikian rupa untuk menarik perhatian dan menumbuhkan kepercayaan korban terhadap informasi yang pada kenyataannya tidak benar. Oleh karena itu, dapat disimpulkan bahwa platform media daring memiliki tingkat kerentanan yang tinggi terhadap praktik penipuan (Tuju et al., 2025).

Penipuan *online* di Indonesia menglami kenaikan yang konsisten setiap tahun, seiring dengan semakin besarnya penggunaan internet dan layanan digital oleh masyarakat. Menurut laporan resmi dari Kepolisian Negara Republik Indonesia, Kementerian Komunikasi dan Informatika, serta Otoritas Jasa Keuangan, penipuan *online* berada di urutan teratas dalam kategori kejahatan siber yang paling sering dilaporkan oleh masyarakat. Fenomena ini menunjukkan pergeseran kejahatan dari lingkungan fisik ke ranah digital, yang sejalan dengan perubahan dalam kebiasaan aktivitas sehari-hari masyarakat (Kementerian Komunikasi dan Digital, 2023).

Tabel 1. Data Laporan Penipuan *Online* di Indonesia (2020–2024).

Tahun	Jumlah Laporan	Sumber Data
2020	±4.500 laporan	Polri & Kominfo
2021	±6.200 laporan	Polri & Kominfo
2022	±8.800 laporan	Polri & Kominfo
2023	±11.400 laporan	Polri & Kominfo
2024	±14.000 laporan	Polri, OJK & Kominfo

Sumber : (Kementerian Komunikasi dan Informatika Republik Indonesia, 2024)

Dengan jumlah laporan yang mengalami Peningkatan sudah jelas menunjukkan bahwa kejahatan semakin sering terjadi, namun juga menunjukkan bahwa masyarakat semakin sadar akan pentingnya melaporkan tindak pidana penipuan *online*. Meski demikian, angka laporan yang tinggi juga menunjukkan bahwa upaya pencegahan dan penanggulangan saat ini belum cukup berhasil dalam mengurangi kejahatan jenis ini.

Modus Operandi Penipuan *Online*

Motivasi utama dalam praktik *carding* berorientasi pada perolehan keuntungan ekonomi, baik dalam bentuk uang maupun barang. Tindak kejahatan ini dapat dilakukan secara individual maupun melalui kerja sama dalam suatu kelompok. Dalam pelaksanaannya, *carding* berlangsung melalui serangkaian tahapan yang terstruktur. Tahap awal meliputi penentuan sarana atau lokasi akses internet yang akan digunakan, kemudian dilanjutkan dengan pemilihan target atau korban. Setelah itu, pelaku mencari data kartu kredit yang akan disalahgunakan, diikuti dengan penerapan metode tertentu untuk melakukan transaksi pembelian. Selanjutnya, pelaku berupaya menembus atau menghindari sistem keamanan yang dimiliki korban agar transaksi dapat diproses tanpa hambatan. Dalam Kamus Besar Bahasa Indonesia, modus operandi merupakan teknik yang dilakukan oleh pelaku kejahatan saat menjalankan aksinya. Penipuan *online* dilakukan dengan berbagai modus yang terus berkembang seiring adanya inovasi teknologi dan kreativitas pelaku kejahatan. Modus yang diterapkan oleh pelaku kejahatan menunjukkan variasi yang beragam, mulai dari modus penjualan barang hingga modus penawaran jasa fiktif kepada korban, dengan memanfaatkan media sosial sebagai sarana utama dalam menjalankan aksinya (Wahyudin et al., 2024).

Carding merupakan tindakan ilegal yang melibatkan penyalahgunaan kartu kredit dengan tujuan memperoleh keuntungan finansial. Dalam praktiknya, pelaku kejahatan umumnya menggunakan kartu kredit tersebut untuk membeli produk berupa hadiah prabayar (Manaf, 2023). Kejahatan ini dilakukan agar pelaku bisa menggunakan kartu kredit orang lain

untuk berbelanja tanpa izin atau mengambil uang milik pemilik kartu tersebut. Pelaku *carding* dalam melakukan aksinya menggunakan media kartu kredit, yang merupakan alat pembayaran yang semakin banyak digunakan oleh masyarakat di dunia, termasuk Indonesia. Perkembangan penggunaan kartu kredit ini didorong oleh beberapa faktor, seperti kemudahan, kepraktisan, serta citra diri yang didapat oleh pemegang kartu.

Beberapa modus operandi yang dapat dilakukan dengan menggunakan kartu kredit antara lain :

1) *Fraud application*, atau yang sering disebut penipuan aplikasi, adalah cara untuk menipu dengan memberikan informasi palsu saat mengajukan suatu layanan atau aplikasi (Putri et al., 2024). Tujuannya adalah agar pengajuan tersebut disetujui meskipun sebenarnya tidak memenuhi syarat. Penipuan ini sering terjadi dalam pengajuan pinjaman online, kartu kredit, asuransi, pembukaan rekening, atau layanan digital lainnya. Pelaku biasanya memalsukan identitas, dokumen, penghasilan, alamat, atau menggunakan data orang lain tanpa izin. Akibatnya bisa berupa kerugian finansial, penyalahgunaan data pribadi, serta meningkatnya risiko kejahatan siber.
2) *Non recived card* adalah bentuk penipuan atau masalah dalam layanan perbankan di mana nasabah mengatakan bahwa mereka tidak menerima kartu(seperti kartu debit atau kartu kredit) yang sebenarnya sudah dicetak dan dikirim oleh bank (Ramadhan et al., 2024). Dalam beberapa kejadian, kartu tersebut dibawa pergi atau digunakan oleh orang lain selama pengiriman, atau digunakan oleh pelaku penipuan yang bekerja sama dengan pihak tertentu. Akibatnya, kartu bisa digunakan untuk melakukan transaksi ilegal sebelum nasabah menyadari hal tersebut, sehingga menyebabkan kerugian finansial dan risiko terhadap data pribadi. Untuk mencegah hal ini, proses pengiriman kartu harus diawasi dengan ketat dan dilakukan verifikasi yang memadai sebelum kartu diaktifkan.
3) *Lost/Stolen Card* terjadi ketika seseorang menggunakan kartu kredit asli yang hilang atau dicuri dari pemiliknya yang sah. Saat melakukan transaksi, pelaku menandatangani slip pembelian (*sales draft*) dengan meniru tanda tangan yang tertera di kartu atau tanda tangan pemegang kartu sebenarnya. Agar transaksi tidak terdeteksi, pelaku sering kali melakukan pembelian dengan nilai di bawah batas maksimal (*floor limit*), sehingga tidak memerlukan persetujuan dari pihak penerbit kartu. Cara ini memanfaatkan ketidaktahuan atau kelengahan dari pemilik kartu,

toko yang menerima pembelian, serta sistem pengawasan transaksi. Akibatnya, pemegang kartu dan pihak penerbit bisa mengalami kerugian finansial.

4) *Altered Card* Kartu yang sudah diubah, menggunakan kartu kredit asli yang telah dimodifikasi datanya. Pelaku menggunakan kartu yang dicuri dan kartu bantuan (*relief*) yang dipanaskan dan dibuat rata, kemudian diberi data baru melalui reembossed. Sementara itu, strip magnetik diisi dengan data baru yang telah dienkripsi kembali dari titik kompromi (POC).
5) *Totally counterfeilted*, dalam konteks penipuan berarti sesuatu dibuat sepenuhnya palsu, sehingga tampak dan berfungsi seperti aslinya. Dalam kasus penipuan perbankan atau kartu, totally counterfeited berarti seluruh bagian kartu atau alat pembayaran dibuat dari awal, mulai dari bentuk fisik, nomor, logo, hingga data elektroniknya. Berbeda dengan pemalsuan sebagian, totally counterfeited tidak memiliki bagian asli dari produk atau dokumen yang ditiru, karena pelakunya membuat tiruan sepenuhnya dari awal dengan meniru semua karakteristik asli (Simanungkalit et al., 2024).
6) *White plastic card*, adalah kartu berbahan plastik yang bentuknya mirip dengan kartu kredit atau kartu debit, tetapi tidak memiliki logo bank, nama penerbit, atau desain resmi (Agustin et al., 2023). Dalam penelitian akademik dan jurnal yang membahas kejahatan perbankan, istilah kartu plastik putih digunakan untuk menyebut kartu kosong berbahan PVC yang digunakan sebagai alat untuk meng-*copy* data kartu asli. Kartu ini memiliki ukuran sama dengan kartu pembayaran biasa dan dilengkapi dengan strip magnetik yang bisa diisi ulang dengan data pemegang kartu yang sah, seperti nomor kartu dan informasi lainnya, yang didapatkan secara tidak sah.
7) Pemalsuan rekam penjualan (ROC) adalah salah satu cara penipuan dalam proses pembayaran, terutama dalam transaksi menggunakan kartu kredit atau sistem pembayaran tanpa uang tunai. ROC adalah buku catatan atau dokumen elektronik yang mencatat detail transaksi penjualan, seperti tanggal, jumlah uang yang dikeluarkan, nomor kartu yang digunakan, serta informasi tentang penjual (Novriano et al., 2022). Dalam kasus pemalsuan, seseorang sengaja mengubah, membuat palsu, atau memanipulasi dokumen tersebut agar tidak sesuai dengan kenyataan, seperti menambah jumlah pembayaran, menggandakan transaksi yang sudah ada, atau membuat transaksi yang tidak benar-benar terjadi
8) *Altered amount* adalah penipuan kartu kredit di mana nilai transaksi diubah atau dimanipulasi oleh orang yang tidak bertanggung jawab setelah pemilik kartu telah

melakukan pembayaran secara sah. Perubahan ini sering terjadi pada struk belanja atau bukti transaksi, seperti menambahkan angka nol atau mengubah jumlah transaksi yang kecil menjadi lebih besar (Lalamentik, 2020). Akibatnya, jumlah yang dibebankan kepada pemilik kartu menjadi lebih tinggi dari yang sebenarnya, sehingga menyebabkan kerugian finansial. Modus ini biasanya terjadi karena kurangnya pengawasan, verifikasi tanda tangan, atau ketelitian dalam mencatat transaksi, sehingga memerlukan pengawasan dan pemeriksaan ulang transaksi yang ketat dari pihak *merchant* dan bank.

9) *Telephone/mail order* (TMO) merupakan salah satu bentuk penipuan kartu kredit yang dilakukan tanpa kehadiran fisik pelaku atau pemegang kartu. Modus ini dilakukan dengan memesan barang atau jasa melalui telepon atau surat dengan menggunakan data kartu kredit milik orang lain yang telah diperoleh sebelumnya, seperti nama pemilik kartu, nomor kartu, dan tanggal kedaluwarsa. Dalam transaksi ini, pemalsu tidak memerlukan kartu fisik karena proses pembayaran dilakukan secara *card-not-present transaction*. Verifikasi hanya didasarkan pada data yang diberikan oleh pemesan, sehingga membuat modus TMO rentan disalahgunakan untuk kejahatan penipuan kartu kredit (Nguyen, 2022).
10) Mengubah program *Electronic Data Capture* (EDC) adalah salah satu cara penipuan dalam transaksi online. Penipu melakukan hal ini dengan memperbaiki, mengubah, atau memasukkan kode ke dalam perangkat lunak pada mesin EDC agar proses transaksi tidak berjalan dengan baik. EDC adalah alat yang digunakan oleh para pedagang untuk memproses pembayaran non tunai, seperti kartu debit dan kartu kredit, dengan cara membaca data dari kartu dan mengirimkannya ke sistem bank (Kartona et al., 2024). Ketika program EDC diubah secara ilegal, penipu bisa mengendalikan proses transaksi, mencuri data dari kartu, atau mengalihkan uang tanpa tahu oleh pemilik kartu maupun pihak bank.
11) Identitas pelaku usaha fiktif, penipuan ini merujuk pada pelaku usaha yang memalsukan data akun pada saat proses pendaftaran. Akun tersebut umumnya belum melalui tahap verifikasi oleh platform jual beli daring, sehingga identitas pelaku usaha menjadi sulit dilacak karena informasi yang dicantumkan, seperti nama, alamat, maupun kontak, tidak sesuai dengan data yang sebenarnya (Mulyadi et al., 2024). Pelaku membuat akun merchant dengan menggunakan identitas dan dokumen yang tidak benar atau meminjam identitas orang lain, lalu melakukan transaksi palsu

tanpa ada proses jual beli barang atau jasa yang nyata. Tujuan dari tindakan ini adalah untuk mengambil dana secara tidak sah.

Tabel 2. Jenis Modus Penipuan *Online* yang Paling Banyak Dilaporkan.

No	Modus Penipuan	Karakteristil Utama
1	Jual beli *online* fiktif	Barang tidak dikirim setelah pembayaran
2	Investasi bodong digital	Janji keuntungan tinggi dalam waktu singkat
3	*Phishing*	Pencurian data melalui tautan palsu
4	Penyamaran Identitas	Mengaku sebagai instansi/perorangan terpercaya

Sumber : (Kementerian Komunikasi dan Digital, 2023)

Secara umum, variasi cara penipuan online seperti yang terlihat dalam tabel tersebut menunjukkan bahwa penipuan online adalah kejahatan yang selalu berubah dan menyesuaikan diri. Cara-cara tersebut tidak hanya berkembang secara teknis, tetapi juga memanfaatkan pola pikir dan kondisi sosial korban. Hal ini menunjukkan bahwa mengatasi penipuan online tidak hanya bisa dilakukan dengan hukum semata, tetapi juga memerlukan upaya pencegahan dengan meningkatkan pemahaman tentang dunia maya, pengetahuan keuangan, serta memperkuat pengawasan di dunia maya.

5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa penipuan online merupakan bentuk kejahatan siber yang berkembang pesat seiring kemajuan teknologi informasi dan komunikasi, dengan modus yang semakin beragam seperti phishing, investasi bodong digital, dan penyamaran identitas. Berdasarkan analisis kriminologis, faktor utama penyebab kejahatan ini tidak hanya terletak pada lemahnya penegakan hukum, tetapi juga pada aspek sosial dan perilaku masyarakat yang mudah terpengaruh oleh bujukan digital serta rendahnya kesadaran keamanan siber. Pendekatan hukum yang bersifat represif belum cukup efektif tanpa didukung peningkatan literasi digital dan pengawasan sosial. Oleh karena itu, penipuan online perlu dipahami sebagai fenomena sosial yang kompleks yang menuntut kerja sama lintas sektor antara aparat hukum, lembaga keuangan, dan masyarakat untuk mencegah serta menekan angka kejahatan siber.

Berdasarkan hasil penelitian ini, disarankan agar pemerintah dan aparat penegak hukum memperkuat upaya pencegahan melalui peningkatan literasi digital masyarakat serta pengawasan terhadap aktivitas daring yang berpotensi menimbulkan tindak penipuan. Lembaga pendidikan dan media juga diharapkan berperan aktif dalam memberikan edukasi publik mengenai keamanan digital dan etika berinternet. Selain itu, penelitian selanjutnya perlu

memperluas fokus pada aspek psikologis pelaku dan korban serta efektivitas kebijakan hukum yang ada, agar dapat memberikan dasar empiris bagi pengembangan strategi pencegahan yang lebih komprehensif di masa mendatang.

DAFTAR PUSTAKA

Agustin, L., Marliyah, & Wahyu, S. (2023). Pengaruh intensitas penggunaan kartu plastik dan mobile payment terhadap consumer behavior: Studi kasus mahasiswa FEBI UINSU. Sci-Tech Journal, 2(2), 166–188. https://doi.org/10.56709/stj.v2i2.77

Amelia. (2023). Kajian hukum terhadap tindak pidana penipuan secara online. Jurnal Inovasi Global, 1(1), 14–25. https://jig.rivierapublishing.id/index.php/rv/index

Butarbutar, R. (2023). Kejahatan siber terhadap individu: Jenis, analisis, dan perkembangannya. Technology and Economics Law Journal, 2(2). https://doi.org/10.21143/telj.vol2.no2.1043

Kartona, Y. F., Kiak, N. T., & Tiwu, M. I. H. (2024). Analisis penggunaan mesin electronic data capture (EDC) pada wajib pajak restoran sebagai upaya mengoptimalkan penerimaan pajak daerah di Kota Kupang. Inisiatif: Jurnal Ekonomi, Akuntansi dan Manajemen, 3(3), 244–260. https://doi.org/10.30640/inisiatif.v3i3.2753

Kementerian Komunikasi dan Digital. (2023, February 14). Siaran pers No. 16/HM/KOMINFO/02/2023 tentang pemerintah usulkan tujuh materi rancangan perubahan kedua UU ITE. https://www.komdigi.go.id/berita/siaran-pers/detail/siaran-pers-no-16-hm-kominfo-02-2023-tentang-pemerintah-usulkan-tujuh-materi-rancangan-perubahan-kedua-uu-ite

Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). Laporan tahunan kamsiber 2024. https://csirt.komdigi.go.id

Kustiawan, W., Harahap, D. K., Jannah, N. A., Sinaga, W. A., Safika, N., Lubis, H. A., & Al Barry, A. A. (2022). Media online dan perkembangannya. Maktabatun: Jurnal Perpustakaan dan Informasi, 2(1).

Lalamentik, S. J. (2020). Penerapan hukum bagi pelaku penyalahgunaan kartu kredit (fraud) menurut KUHPidana. Lex Crimen, 9(1).

Lubis, M. R., Siregar, G. T. P., Fraya, V., Nasution, H., & Lubis, D. (2023). Peningkatan kesadaran hukum masyarakat: Memahami perbedaan tindak pidana penipuan dan penggelapan. Bulletin of Community Engagement, 3(2). https://attractivejournal.com/index.php/bce/

Manaf, I. (2023). Analysis of carding crime as a form of cyber crime in Indonesian criminal law. JLASA (Journal of Law and State Administration), 1(1), 1–7.

Mulyadi, Nurdin, A. A., Anjani, A. A., Alamsyah, F. D., Sifana, F., Yudistio, M. A., Kareem, M. M., & Rabbani, R. A. A. (2024). Analisis penipuan online melalui media sosial

dalam perspektif kriminologi. Media Hukum Indonesia (MHI), 2(2), 74. https://doi.org/10.5281/zenodo.11183088

Nguyen, T. V. (2022). The modus operandi of transnational computer fraud: A crime script analysis in Vietnam. Trends in Organized Crime, 25(2), 226–247. https://doi.org/10.1007/s12117-021-09422-1

Novriano, F., Makarao, T., & Mawadi, H. (2022). Penegakan hukum tindak pidana peretasan data pribadi konsumen kartu kredit menurut Undang-Undang Informasi dan Transaksi Elektronik Nomor 19 Tahun 2016. Jurisdictie, 4(2), 167–190.

Nur, F. (2025). Pertanggungjawaban pidana terhadap pelaku tindak pidana penipuan online dengan modus social engineering. Innovative: Journal of Social Science Research, 3(4), 342–355. https://j-innovative.org/index.php/Innovative

Patroli Siber. (2025). Jumlah laporan polisi yang dibuat masyarakat. https://patrolisiber.id/statistic

Putri, D. E., Sudarti, E., & Siregar, E. (2024). Tindak pidana penipuan melalui aplikasi digital (gagasan pemikiran pertanggungjawaban oleh bank). PAMPAS: Journal of Criminal Law, 5(1). https://journal.unismuh.ac.id/index.php/jhes/article/view/2419/2357

Ramadhan, M. A., Anggoro, J. I., & Susanto, M. (2024). Analisis penyalahgunaan perbankan dalam rangka mengidentifikasi kerugian ekonomi dan upaya pencegahannya. Jurnal Media Akademik (JMA), 2(2). https://doi.org/10.62281

Rantesalu, H. (2022). Penanggulangan kejahatan penipuan belanja online di wilayah Kepolisian Daerah Jawa Timur. Janaloka Jurnal, 1(2), 70–94.

Ratulangi, H. C., Wahongan, A. S., & Mewengkang, F. R. (2021). Tindak pidana cyber crime dalam kegiatan perbankan. Lex Privatum, 9(5).

Simanungkalit, J. A. R., Hertadi, R., & Hosnah, A. U. (2024). Analisis tindak pidana penipuan online dalam konteks hukum pidana: Cara menanggulangi dan pencegahannya. Jurnal Mahasiswa Humanis, 4(2), 281–294.

Situmeang, S. M. T. (2021). Buku ajar kriminologi. PT Rajawali Buana Pusaka.

Tuju, M. C., Ramadani, S., & Nasution, C. (2025). Penegakan hukum terhadap tindak pidana siber dalam kasus penipuan jual beli online dalam perspektif kriminologi. Innovative: Journal of Social Science Research, 5(2), 1763–1776. https://j-innovative.org/index.php/Innovative

Wahyudi, D., Samosir, H. S., & Devi, R. S. (2022). Akibat hukum bagi pelaku tindak pidana penipuan online melalui modus arisan online di media sosial elektronik. Jurnal Rectum, 4(2), 326–336.

Wahyudin, J., Renggong, R., & Hamid, A. H. (2024). Analisis tindak pidana penipuan secara online di wilayah Kepolisian Daerah Sulawesi Selatan. Indonesian Journal of Legality of Law, 6(2), 273–282. https://doi.org/10.35965/ijlf.v6i2.4474

Waskito, H. B., & Nurhadiyanto, L. (2020). Analisis cyberbullying pada remaja berbasis routine activity theory di media sosial Instagram. Jurnal Anomie, 2(1), 1–19.