Jurnal Cendekia Hukum Indonesia
Vol. 2 No. 2 Tahun 2026
Licensed CC BY-SA 4.0, Hal 194-215
DOI: https://doi.org/10.71417/jchi.v2i2236.
https://hukum.journalpustakacendekia.com/index.php/JCHI

Tinjauan Yuridis Penyalahgunaan Media Elektronik dalam Tindak Pidana Penipuan (Studi pada Unit Cyber Polda Kalimantan Timur)

Najwa Nurul Aulia[1], Iskandar Yusuf[2]
[1]Hukum Pidana Islam, Sekolah Tinggi Agama Islam Balikpapan, Kalimantan Timur.
[2]Hukum Pidana Islam, Sekolah Tinggi Agama Islam Balikpapan, Kalimantan Timur.
Email correspondence: najwanurulaulia28@gmail.com

Abstract. *The rapid use of electronic media has expanded the methods, reach, and speed of fraud. This study examines the legal qualification of electronic-media abuse in fraud and evaluates law enforcement practices associated with the Cyber Unit of the East Kalimantan Regional Police. The study applies a limited empirical juridical design using statutory, case, and conceptual approaches. Data were obtained from current legislation, official police and financial-sector releases, and relevant legal studies. The analysis shows that general fraud is governed by Article 492 of Law Number 1 of 2023 on the Criminal Code, while Article 28 paragraph (1) of the Electronic Information and Transactions Law applies more specifically when misleading electronic information causes material loss to consumers in an electronic transaction. Account hacking, data manipulation, or unlawful access may activate other provisions of the same law. Electronic evidence now receives express recognition under Law Number 20 of 2025 on Criminal Procedure, but its admissibility depends on authenticity and lawful acquisition. Enforcement is constrained by false identities, mule accounts, cross-border infrastructure, delayed reporting, limited forensic resources, and fragmented cooperation. Effective enforcement requires rapid evidence preservation, accountable digital forensics, coordinated account blocking, and stronger victim-oriented procedures.*

Keywords: *Electronic Media; Fraud; Electronic Evidence; Cyber Crime; Law Enforcement.*

Abstrak. Penggunaan media elektronik memperluas modus, jangkauan, dan kecepatan tindak pidana penipuan. Penelitian ini bertujuan mengkaji kualifikasi yuridis penyalahgunaan media elektronik dalam penipuan serta menilai praktik penegakan hukum yang berkaitan dengan Unit Cyber Polda Kalimantan Timur. Penelitian memakai desain yuridis empiris terbatas dengan pendekatan perundang-undangan, kasus, dan konseptual. Data bersumber dari peraturan yang berlaku, rilis resmi kepolisian dan sektor keuangan, serta penelitian hukum yang relevan. Hasil kajian menunjukkan bahwa penipuan umum tunduk pada Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang KUHP. Pasal 28 ayat (1) UU ITE berlaku lebih khusus ketika informasi elektronik yang menyesatkan menimbulkan kerugian materiel bagi konsumen dalam Transaksi Elektronik. Peretasan akun, manipulasi data, atau akses tanpa hak dapat dikenai ketentuan lain dalam UU ITE. Bukti elektronik telah diakui secara tegas dalam Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP, tetapi keabsahannya bergantung pada autentikasi dan cara perolehan yang tidak melawan hukum. Penegakan hukum masih terhambat identitas palsu, rekening penampung, infrastruktur lintas negara, keterlambatan laporan, keterbatasan forensik, dan koordinasi yang belum cepat.

Kata Kunci: Media Elektronik; Penipuan; UU ITE; Bukti Elektronik; Penegakan Hukum.

Received Juli 26, 2026; Revised Juli 27, 2026; Accepted Juli 27, 2026
Najwa Nurul Aulia[1], Iskandar Yusuf[2], najwanurulaulia28@gmail.com

LATAR BELAKANG

Perkembangan teknologi informasi telah memindahkan banyak kegiatan ekonomi, komunikasi, dan pelayanan ke ruang elektronik. Masyarakat melakukan transaksi, menyimpan identitas, mengirim dokumen, serta membangun relasi melalui telepon seluler, media sosial, aplikasi pesan, dan *marketplace*. Perubahan ini memberi manfaat yang nyata. Namun, perubahan yang sama juga memberi pelaku sarana untuk menjangkau korban secara cepat, menyembunyikan identitas, memindahkan hasil kejahatan, dan menghapus jejak digital. Penipuan tidak lagi selalu terjadi melalui pertemuan langsung. Pelaku dapat membuat akun palsu, meniru identitas pihak tepercaya, mengirim tautan *phishing*, menawarkan investasi fiktif, atau mengambil alih akun media sosial korban.

Skala masalah tersebut terlihat dari data Indonesia Anti-Scam Centre. Otoritas Jasa Keuangan mencatat 74.243 laporan sampai 23 Maret 2025. Laporan itu berkaitan dengan 78.041 rekening, sedangkan 33.857 rekening telah diblokir. Kerugian yang dilaporkan mencapai Rp1,4 triliun dan dana yang berhasil diblokir sebesar Rp133,2 miliar (Otoritas Jasa Keuangan, 2025). Pada Januari 2026, Otoritas Jasa Keuangan menyatakan bahwa IASC telah mengembalikan Rp161 miliar kepada 1.070 korban melalui koordinasi dengan 14 bank. Modus yang sering muncul meliputi penipuan belanja, panggilan palsu, investasi, pekerjaan, media sosial, dan *love scam* (Otoritas Jasa Keuangan, 2026). Data tersebut menunjukkan bahwa penanganan penipuan digital tidak cukup hanya berorientasi pada penangkapan pelaku. Aparat juga harus bergerak cepat untuk mempertahankan bukti, memutus akses terhadap rekening, dan memulihkan kerugian korban.

Kalimantan Timur menghadapi pola yang serupa. Subdirektorat V Siber Direktorat Reserse Kriminal Khusus Polda Kalimantan Timur mengingatkan masyarakat tentang modus *phishing* melalui pesan langsung, penyamaran sebagai petugas bank atau layanan pelanggan, pekerjaan fiktif, dan manipulasi untuk memperoleh data perbankan. Rilis resmi Polda Kalimantan Timur juga menyebut peningkatan kasus penipuan *online* dari 2024 ke 2025 serta temuan investasi ilegal yang menjanjikan keuntungan harian yang tidak wajar (Polda Kalimantan Timur, 2025). Pada perkara lain, penyidik mengungkap pelaku yang mengambil nomor telepon calon pembeli dari komentar siaran langsung Facebook, lalu menyamar sebagai admin toko untuk meminta pembayaran. Perkara

tersebut menunjukkan bahwa satu rangkaian penipuan dapat memuat pemalsuan identitas, manipulasi informasi elektronik, dan pemindahan uang (Polda Kalimantan Timur, 2024).

Media elektronik memberi karakter khusus pada penipuan. Pertama, pelaku dapat memakai identitas yang tidak sesuai dengan identitas hukum. Kedua, bukti utama sering berbentuk percakapan, rekaman panggilan, alamat internet, data akun, catatan transaksi, metadata, dan informasi perangkat. Ketiga, pelaku dapat menggunakan rekening pinjaman atau *money mule* sehingga aliran dana tidak langsung menunjukkan pelaku utama. Keempat, sebagian data berada dalam penguasaan bank, penyelenggara sistem elektronik, operator telekomunikasi, atau penyedia layanan yang berlokasi di luar negeri. Karakter ini menuntut penyidikan yang cepat, teknis, dan tetap tunduk pada hukum acara.

Secara yuridis, istilah penipuan melalui media elektronik tidak selalu menunjuk satu pasal tunggal. Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana mengatur penipuan umum. Pasal ini berlaku sejak 2 Januari 2026. Sementara itu, Pasal 28 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE mengatur penyebaran atau transmisi informasi elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang menimbulkan kerugian materiel bagi konsumen dalam Transaksi Elektronik. Rumusan tersebut tidak mencakup seluruh bentuk penipuan *online*. Unsur konsumen dan Transaksi Elektronik harus terbukti. Apabila perbuatan melibatkan pengambilalihan akun, akses tanpa hak, atau manipulasi data agar tampak autentik, penyidik perlu menilai ketentuan lain dalam UU ITE.

Perubahan hukum acara juga memengaruhi penanganan perkara. Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana berlaku sejak 2 Januari 2026 dan mencabut Undang-Undang Nomor 8 Tahun 1981. KUHAP baru mengakui bukti elektronik sebagai alat bukti tersendiri. KUHAP baru juga mensyaratkan autentikasi dan perolehan alat bukti yang tidak melawan hukum. Pengaturan ini memperkuat kedudukan bukti digital, tetapi sekaligus meningkatkan kewajiban penyidik untuk menjaga integritas data, legalitas penggeledahan, legalitas penyitaan, dan dokumentasi proses forensik.

Penelitian terdahulu telah mengkaji penipuan *online*, bukti elektronik, dan hambatan penyidikan. Zahrulswendar et al. (2021) menegaskan bahwa ketentuan penipuan dalam UU ITE memiliki ruang lingkup yang lebih sempit daripada penipuan umum karena

berorientasi pada kerugian konsumen dalam transaksi elektronik. Rahmawati et al. (2022) menunjukkan kebutuhan pelatihan siber bagi penyidik dan edukasi publik dalam perkara penipuan bermodus giveaway. Fitriati et al. (2022) menemukan hambatan berupa penghapusan log, keterlambatan diketahui korban, serta kebutuhan kerja sama lintas negara dan dukungan ahli telematika. Sanjaya et al. (2022) menekankan bahwa akun media sosial dapat menjadi sumber bukti elektronik sepanjang relevansi dan keasliannya dapat dipertanggungjawabkan.

Kajian tersebut memberi dasar penting, tetapi perubahan hukum pada 2024 sampai 2026 memerlukan analisis baru. KUHP nasional telah berlaku. KUHAP baru telah mengatur bukti elektronik secara eksplisit. Undang-Undang Nomor 1 Tahun 2026 juga menyesuaikan ancaman pidana di luar KUHP dengan sistem kategori denda. Selain itu, praktik Unit Cyber Polda Kalimantan Timur memperlihatkan pola lokal yang penting, seperti penyamaran admin toko, *phishing*, investasi ilegal, dan pelacakan pelaku lintas daerah. Oleh karena itu, penelitian ini memusatkan perhatian pada hubungan antara norma yang berlaku, karakter bukti digital, tahapan penanganan perkara, dan faktor penghambat penegakan hukum.

Penelitian ini menjawab empat pertanyaan. Pertama, bagaimana bentuk penyalahgunaan media elektronik dalam tindak pidana penipuan. Kedua, bagaimana tahapan penegakan hukum yang relevan bagi Unit Cyber Polda Kalimantan Timur. Ketiga, faktor apa yang menghambat penyidikan dan pemulihan kerugian korban. Keempat, apakah penerapan KUHP, UU ITE, dan KUHAP baru telah memberi dasar yang memadai untuk pertanggungjawaban pidana pelaku dan perlindungan korban. Tujuan penelitian ialah menghasilkan analisis yuridis yang tepat, membatasi penerapan setiap pasal secara jelas, dan merumuskan langkah perbaikan yang dapat diterapkan oleh penyidik serta lembaga pendukung.

METODE PENELITIAN

Penelitian ini menggunakan desain yuridis empiris terbatas. Penelitian menelaah hukum sebagai norma sekaligus menilai penerapannya melalui data publik mengenai penanganan perkara siber di Kalimantan Timur. Pendekatan yang digunakan terdiri atas pendekatan perundang-undangan (*statute approach*), pendekatan kasus (*case approach*), dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan

dipakai untuk menguji unsur tindak pidana, kewenangan penyidik, alat bukti, upaya paksa, dan hak korban. Pendekatan kasus dipakai untuk membaca pola perbuatan yang muncul dalam rilis resmi Polda Kalimantan Timur. Pendekatan konseptual dipakai untuk menjelaskan penipuan, bukti elektronik, pertanggungjawaban pidana, dan efektivitas penegakan hukum.

Lokasi kajian diarahkan pada Unit Cyber atau Subdirektorat V Siber Direktorat Reserse Kriminal Khusus Polda Kalimantan Timur. Bahan hukum primer meliputi Undang-Undang Nomor 1 Tahun 2023 tentang KUHP, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE, Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP, dan Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana. Data empiris awal berasal dari rilis resmi Polda Kalimantan Timur dan publikasi resmi Otoritas Jasa Keuangan mengenai bentuk perkara, pola penipuan, pemblokiran rekening, serta pengembalian dana korban. Bahan sekunder berasal dari buku dan artikel jurnal yang membahas penipuan *online*, penyidikan siber, alat bukti elektronik, dan penegakan hukum.

Teknik pengumpulan data memakai studi kepustakaan dan dokumentasi. Peneliti menginventarisasi norma yang berlaku, mengelompokkan unsur delik, mencatat perubahan ketentuan sejak 2024 sampai 2026, lalu menghubungkannya dengan pola perkara yang tersedia dalam sumber resmi. Analisis dilakukan secara kualitatif dengan metode deskriptif-analitis. Setiap modus dinilai berdasarkan perbuatan, tujuan pelaku, kedudukan korban, media yang digunakan, bentuk kerugian, dan jenis bukti yang dapat ditemukan. Setelah itu, penelitian menentukan ketentuan pidana yang paling sesuai dan menilai prosedur pembuktiannya.

Landasan teori penelitian memakai teori penegakan hukum Soerjono Soekanto. Menurut Soekanto (2019), efektivitas penegakan hukum dipengaruhi oleh lima faktor, yaitu faktor hukum, aparat penegak hukum, sarana dan prasarana, masyarakat, serta kebudayaan. Faktor hukum menyangkut kejelasan dan keselarasan norma. Faktor aparat menyangkut kompetensi, integritas, koordinasi, dan diskresi. Faktor sarana menyangkut laboratorium, perangkat, anggaran, akses data, dan dukungan ahli. Faktor masyarakat menyangkut kesadaran melapor, kemampuan menjaga bukti, serta kepatuhan terhadap prosedur. Faktor kebudayaan menyangkut nilai, kebiasaan, dan pola perilaku digital yang memengaruhi keberhasilan penegakan hukum.

Teori tersebut digunakan karena penipuan melalui media elektronik tidak dapat dijelaskan hanya dari ketersediaan pasal. Norma yang jelas tidak akan efektif ketika korban terlambat melapor, penyidik tidak memperoleh data dari *platform*, rekening telah dikosongkan, atau bukti digital berubah. Sebaliknya, dukungan teknologi tidak dapat membenarkan penggeledahan dan penyitaan yang melanggar prosedur. Penegakan hukum yang efektif harus mempertemukan ketepatan norma, kompetensi penyidik, sarana forensik, partisipasi masyarakat, dan budaya keamanan digital.

Naskah ini tidak mengklaim hasil wawancara penyidik karena transkrip wawancara dan salinan berkas perkara belum diberikan kepada penyusun. Uraian praktik lapangan dibatasi pada informasi yang telah dipublikasikan oleh lembaga resmi. Untuk pengajuan sebagai artikel hasil penelitian lapangan, peneliti perlu menambahkan wawancara semi-terstruktur dengan penyidik Unit Cyber, petugas digital forensik, dan pihak yang menangani pelacakan transaksi. Peneliti juga perlu memeriksa dokumen perkara setelah memperoleh izin. Langkah tersebut penting untuk memvalidasi waktu penanganan, kendala akses data, kualitas sarana, dan hasil pemulihan aset.

HASIL DAN PEMBAHASAN

A. Bentuk Penyalahgunaan Media Elektronik dalam Tindak Pidana Penipuan

1. Kedudukan Media Elektronik dalam Perbuatan Pidana

UU ITE tidak memakai istilah media elektronik sebagai satu kategori delik yang berdiri sendiri. Undang-undang tersebut mengatur Informasi Elektronik, Dokumen Elektronik, Sistem Elektronik, dan Transaksi Elektronik. Dalam penelitian ini, media elektronik dipahami sebagai sarana berbasis sistem elektronik yang dipakai untuk membuat, mengolah, menyimpan, menampilkan, mengirim, atau menyebarkan informasi. Pengertian fungsional ini mencakup telepon seluler, aplikasi pesan, media sosial, *marketplace*, situs web, surat elektronik, rekening digital, dan layanan berbasis internet.

Media elektronik dapat berfungsi sebagai sarana komunikasi, objek serangan, tempat penyimpanan bukti, dan sarana pemindahan hasil kejahatan. Dalam penipuan jual beli, aplikasi pesan dan *marketplace* menjadi sarana menawarkan barang yang tidak ada. Dalam *impersonation scam*, akun dan nomor telepon dipakai untuk meniru lembaga atau orang lain. Dalam pengambilalihan akun, akun korban menjadi objek akses tanpa hak sekaligus alat untuk menipu pengikut korban. Dalam investasi fiktif, media elektronik

membangun tampilan seolah-olah kegiatan usaha memiliki izin, keuntungan, dan transaksi yang sah. Perbedaan fungsi tersebut menentukan pasal yang diterapkan.

2. Bentuk Penyalahgunaan

Bentuk pertama ialah penipuan jual beli *online*. Pelaku menawarkan barang melalui media sosial atau *marketplace*, menggunakan foto milik pihak lain, membuat testimoni palsu, lalu meminta korban mentransfer pembayaran. Setelah pembayaran dilakukan, barang tidak dikirim, barang tidak sesuai, atau akun menghilang. Perbuatan ini memenuhi pola penipuan ketika tipu muslihat atau rangkaian kebohongan menggerakkan korban menyerahkan uang. Apabila korban berkedudukan sebagai konsumen dan hubungan terjadi dalam Transaksi Elektronik, Pasal 28 ayat (1) UU ITE dapat dinilai bersama Pasal 492 KUHP.

Bentuk kedua ialah penyamaran identitas atau *impersonation scam*. Pelaku berpura-pura sebagai petugas bank, layanan pelanggan, admin toko, pejabat, teman, atau anggota keluarga. Pelaku meminta kode autentikasi, data pribadi, pembayaran, atau pemindahan dana. Perkara yang dipublikasikan Polda Kalimantan Timur pada 2024 menunjukkan pelaku memperoleh nomor calon pembeli dari komentar siaran langsung Facebook, lalu menyamar sebagai admin toko. Perbuatan ini tidak hanya berisi kebohongan. Apabila pelaku mengubah, menciptakan, atau memanipulasi Informasi Elektronik agar seolah-olah autentik, ketentuan tentang manipulasi Informasi Elektronik dalam UU ITE dapat diterapkan (Polda Kalimantan Timur, 2024).

Bentuk ketiga ialah investasi bodong. Pelaku menjanjikan keuntungan tinggi, memakai grup pesan, aplikasi, situs, atau akun media sosial untuk menampilkan hasil investasi yang tidak nyata. Korban diminta menambah setoran agar dapat menarik dana. Polda Kalimantan Timur menyebut pola investasi ilegal yang menjanjikan keuntungan sekitar dua persen per hari. Janji tersebut membangun keadaan palsu tentang kegiatan usaha dan kemampuan pembayaran. Analisis yuridis perlu membedakan penipuan biasa, penghimpunan dana tanpa izin, kegiatan jasa keuangan ilegal, dan tindak pidana pencucian uang apabila hasil kejahatan disamarkan.

Bentuk keempat ialah *love scam*. Pelaku membangun hubungan emosional melalui media sosial atau aplikasi perkenalan. Setelah memperoleh kepercayaan, pelaku membuat keadaan darurat palsu, meminta biaya perjalanan, modal, atau pembayaran tertentu. Unsur konsumen dalam Pasal 28 ayat (1) UU ITE tidak selalu terpenuhi karena hubungan

tersebut belum tentu merupakan hubungan konsumen dan pelaku usaha. Oleh sebab itu, Pasal 492 KUHP lebih tepat menjadi dasar utama ketika tipu muslihat menggerakkan korban menyerahkan uang.

Bentuk kelima ialah pengambilalihan akun dan penipuan kepada jaringan korban. Pelaku memperoleh kata sandi melalui *phishing*, pencurian kode autentikasi, atau akses tanpa hak. Setelah menguasai akun, pelaku mengubah data pengamanan dan menghubungi pengikut korban untuk meminta uang. Rangkaian ini dapat memuat beberapa perbuatan, yaitu akses tanpa hak, perubahan data, pemerasan, dan penipuan. Penyidik harus memisahkan setiap perbuatan, menentukan korban pada setiap tahap, serta menghindari penggunaan satu pasal umum untuk menutup seluruh rangkaian.

3. Unsur Tindak Pidana dan Pemilihan Pasal

Pasal 492 KUHP mengatur penipuan umum. Unsurnya meliputi setiap orang, maksud menguntungkan diri sendiri atau orang lain secara melawan hukum, penggunaan nama palsu atau kedudukan palsu, tipu muslihat atau rangkaian kata bohong, serta tindakan menggerakkan orang agar menyerahkan barang, memberi utang, membuat pengakuan utang, atau menghapus piutang. Fokus delik terletak pada hubungan sebab akibat antara sarana penipuan dan tindakan korban yang merugikan dirinya. Penggunaan media elektronik tidak mengubah unsur pokok tersebut. Media elektronik menjelaskan cara pelaku membangun kebohongan dan jenis bukti yang ditinggalkan.

Pasal 28 ayat (1) UU ITE memiliki cakupan yang lebih khusus. Penyidik harus membuktikan bahwa pelaku dengan sengaja mendistribusikan atau mentransmisikan Informasi Elektronik atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan. Perbuatan tersebut harus menimbulkan kerugian materiel bagi konsumen dalam Transaksi Elektronik. Dua batas penting muncul dari rumusan ini. Pertama, korban harus berkedudukan sebagai konsumen. Kedua, kerugian harus berkaitan dengan Transaksi Elektronik. Karena itu, penipuan pertemanan, *love scam*, panggilan keluarga palsu, atau hubungan personal lain tidak otomatis masuk Pasal 28 ayat (1) UU ITE (Zahrulswendar et al., 2021).

Ancaman pidana Pasal 45A ayat (1) setelah penyesuaian berdasarkan Undang-Undang Nomor 1 Tahun 2026 ialah penjara paling lama enam tahun dan/atau denda paling banyak kategori V. Pasal 79 KUHP menentukan denda kategori V sebesar Rp500.000.000,00. Penyesuaian ini penting karena naskah hukum dan artikel sebelum 2

Januari 2026 masih sering menyebut denda paling banyak Rp1.000.000.000,00. Peneliti dan penyidik harus memakai ancaman pidana yang berlaku pada waktu penilaian perkara, dengan tetap memperhatikan asas waktu tindak pidana dan ketentuan peralihan.

Ketentuan UU ITE lain dapat diterapkan berdasarkan bentuk perbuatan. Akses tanpa hak terhadap akun atau sistem perlu dianalisis dengan ketentuan akses ilegal. Perubahan, penciptaan, penghilangan, atau manipulasi Informasi Elektronik agar dianggap seolah-olah data autentik perlu dianalisis dengan ketentuan manipulasi. Penggunaan pasal harus mengikuti fakta, bukan hanya label penipuan *online*. Ketika beberapa delik terjadi dalam satu rangkaian, penuntut umum perlu menilai perbarengan tindak pidana menurut KUHP dan hubungan antara ketentuan umum dengan ketentuan khusus secara *in concreto*.

Pertanggungjawaban pidana juga memerlukan kesalahan. Pelaku harus memiliki kemampuan bertanggung jawab, melakukan perbuatan dengan sengaja sesuai rumusan pasal, dan tidak memiliki alasan pembenar atau pemaaf. Dalam jaringan penipuan, pembagian peran sering terdiri atas pembuat akun, pencari data korban, penghubung, pemilik rekening penampung, penarik dana, dan pengendali. Pemilik rekening tidak dapat langsung dipandang sebagai pelaku utama hanya karena rekeningnya menerima dana. Penyidik perlu membuktikan pengetahuan, kesepakatan, manfaat yang diterima, komunikasi, dan keterlibatan nyata. Bukti aliran dana harus dibaca bersama bukti komunikasi dan bukti perangkat.

B. Penegakan Hukum oleh Unit Cyber Polda Kalimantan Timur

1. Tahapan Penanganan Perkara

Penanganan perkara dimulai dari laporan atau pengaduan masyarakat. Pada tahap awal, petugas perlu mengidentifikasi waktu kejadian, akun yang digunakan, nomor telepon, tautan, rekening tujuan, jumlah kerugian, dan perangkat yang menyimpan bukti. Korban sebaiknya menyerahkan tangkapan layar, riwayat percakapan utuh, bukti transfer, surat elektronik, rekaman panggilan yang diperoleh secara sah, alamat akun, serta perangkat asli apabila diperlukan. Tangkapan layar berguna sebagai petunjuk awal, tetapi pemeriksaan tidak boleh berhenti pada gambar karena gambar dapat dipotong, disunting, atau kehilangan metadata.

Setelah laporan diterima, penyelidik menilai apakah peristiwa mengandung tindak pidana dan menentukan pasal awal. Penilaian harus memeriksa kedudukan korban sebagai konsumen, adanya Transaksi Elektronik, cara pelaku menggerakkan korban, serta

kemungkinan akses tanpa hak atau manipulasi data. Kualifikasi yang tepat sejak awal menentukan arah permintaan data. Perkara jual beli membutuhkan data transaksi dan akun penjual. Perkara pengambilalihan akun membutuhkan log akses, perubahan kredensial, alamat internet, identitas perangkat, dan data pemulihan akun.

Penyidikan berfokus pada pengumpulan alat bukti dan penetapan hubungan antara identitas digital dengan orang tertentu. Penyidik dapat memeriksa saksi, korban, ahli, perangkat, sistem, dan aliran dana. Pasal 43 UU ITE memberi kewenangan khusus untuk meminta informasi dari Penyelenggara Sistem Elektronik, membuat data tertentu tidak dapat diakses, meminta bantuan ahli, dan memerintahkan pemutusan akses sementara terhadap akun media sosial, rekening bank, uang elektronik, atau aset digital. Kewenangan tersebut harus dijalankan bersama KUHAP baru serta tetap melindungi privasi, kerahasiaan, kelancaran layanan publik, dan integritas data.

Digital forensic menjadi bagian penting ketika bukti berada pada telepon, komputer, akun, atau media penyimpanan. Pemeriksaan yang baik mencatat kondisi awal perangkat, pihak yang menyerahkan, waktu penerimaan, metode akuisisi, perangkat lunak dan perangkat keras yang digunakan, nilai hash, hasil ekstraksi, serta setiap perpindahan barang bukti. Catatan tersebut membentuk *chain of custody*. Tujuannya bukan hanya menemukan isi percakapan, tetapi juga membuktikan bahwa data yang diajukan sama dengan data yang diperoleh dan tidak berubah selama proses pemeriksaan. Dewi dan Fahrial (2022) serta Sanjaya et al. (2022) menegaskan pentingnya keaslian, relevansi, dan prosedur perolehan bukti elektronik.

Pelacakan rekening harus berjalan paralel dengan pemeriksaan digital. Dana hasil penipuan sering berpindah dalam waktu singkat melalui beberapa rekening, uang elektronik, aset digital, atau penarikan tunai. Koordinasi cepat dengan bank dan IASC meningkatkan peluang pemblokiran. Otoritas Jasa Keuangan (2026) menyatakan bahwa semakin cepat korban melapor, semakin besar peluang dana dapat dikembalikan. Penyidik tetap harus membedakan pemblokiran administratif untuk mencegah perpindahan dana dengan penyitaan sebagai upaya paksa yang tunduk pada KUHAP.

Pelacakan alamat internet dan data pelanggan membantu menghubungkan aktivitas akun dengan perangkat atau jaringan. Namun, alamat internet tidak selalu menunjukkan pelaku secara langsung. Satu alamat dapat digunakan bersama, berubah secara dinamis, melewati VPN, atau berada di bawah pengelolaan penyedia layanan. Karena itu, alamat

internet harus dikombinasikan dengan waktu akses, data perangkat, nomor pelanggan, lokasi, riwayat login, komunikasi, dan aliran dana. Kesimpulan identitas yang hanya bertumpu pada satu data teknis berisiko menghasilkan salah identifikasi.

Setelah minimal dua alat bukti mendukung dugaan terhadap orang tertentu, penyidik dapat menetapkan tersangka sesuai ketentuan hukum acara. Penyidik kemudian menyelesaikan pemberkasan, berkoordinasi dengan penuntut umum, dan melimpahkan perkara beserta tersangka serta barang bukti setelah berkas dinyatakan lengkap. Dalam perkara lintas daerah, koordinasi dengan kepolisian wilayah lain diperlukan untuk pemeriksaan, penggeledahan, penyitaan, atau penangkapan. Rilis Polda Kalimantan Timur pada 2024 menunjukkan bahwa pelacakan dapat membawa penyidik ke daerah tempat pelaku berada, bukan hanya lokasi korban.

Tahapan tersebut harus berorientasi pada korban. KUHAP baru memberi korban hak untuk memperoleh informasi perkembangan perkara, pendampingan, perlindungan identitas dan keamanan, nasihat hukum, serta mengajukan restitusi. Penanganan penipuan digital perlu menghubungkan proses pidana dengan upaya pemulihan dana. Penangkapan pelaku tanpa pengamanan aset sering membuat putusan pidana tidak memulihkan kerugian korban.

2. Analisis Berdasarkan Faktor Penegakan Hukum

Penerapan teori Soerjono Soekanto menunjukkan bahwa efektivitas penanganan penipuan digital bergantung pada hubungan lima faktor. Ringkasan temuan dan kebutuhan perbaikannya disajikan pada Tabel 1.

Tabel 1 Analisis Faktor Penegakan Hukum dalam Penipuan Digital

Faktor	Temuan Utama	Implikasi Yuridis	Arah Perbaikan
Hukum	KUHP, UU ITE, KUHAP baru, dan UU Penyesuaian Pidana membentuk kerangka yang lebih lengkap, tetapi ruang lingkup Pasal 28 ayat (1) UU ITE tetap terbatas pada konsumen dalam Transaksi Elektronik.	Kesalahan memilih pasal dapat mengaburkan unsur delik dan melemahkan dakwaan.	Susun pedoman kualifikasi perkara berdasarkan modus, korban, transaksi, akses, dan manipulasi data.

Aparat	Penyidik harus memahami hukum pidana, transaksi digital, pembuktian elektronik, aliran dana, dan kerja sama lintas wilayah.	Kompetensi yang tidak merata memperlambat pemeriksaan dan meningkatkan risiko kesalahan prosedur.	Lakukan pelatihan berkala, supervisi perkara, dan tim gabungan penyidik, ahli forensik, serta analis transaksi.
Sarana dan prasarana	Pemeriksaan memerlukan perangkat forensik, penyimpanan aman, akses data, anggaran, dan dukungan ahli.	Keterbatasan alat dapat menghambat autentikasi, ekstraksi data, dan pemulihan bukti yang terhapus.	Perkuat laboratorium, lisensi alat, sistem pencatatan barang bukti, dan kerja sama dengan laboratorium nasional.
Masyarakat	Korban sering terlambat melapor, menghapus percakapan, atau terus berkomunikasi dengan pelaku.	Bukti dan dana dapat hilang sebelum tindakan hukum dilakukan.	Sediakan panduan pelaporan cepat, kanal edukasi, dan prosedur penyimpanan bukti yang mudah dipahami.
Kebudayaan	Kebiasaan membagikan kode autentikasi, mempercayai keuntungan tidak wajar, serta meminjamkan rekening meningkatkan risiko.	Normalisasi perilaku tidak aman memperluas pasar korban dan jaringan money mule.	Bangun budaya verifikasi, keamanan akun, dan penolakan penggunaan rekening oleh pihak lain.

Sumber: Diolah peneliti berdasarkan Soekanto (2019), peraturan yang berlaku, dan dokumen resmi terkait.

Faktor hukum menunjukkan kemajuan karena KUHAP baru menempatkan bukti elektronik sebagai alat bukti tersendiri. Namun, norma materiel tetap memerlukan pemilahan. Pasal 28 ayat (1) UU ITE tidak boleh dipakai sebagai rumusan umum untuk semua penipuan melalui internet. Faktor aparat menuntut kompetensi gabungan. Penyidik harus mampu membaca unsur pidana sekaligus memahami struktur data, penyimpanan log, transaksi bank, dan pola penyamaran identitas. Rahmawati et al. (2022) menunjukkan

bahwa pelatihan siber bagi penyidik menjadi kebutuhan yang konsisten dalam penanganan penipuan *online*.

Faktor sarana dan prasarana menentukan kemampuan autentikasi. Perangkat forensik yang tidak diperbarui dapat gagal membaca perangkat baru atau aplikasi terenkripsi. Keterbatasan penyimpanan juga berisiko merusak tata kelola barang bukti. Faktor masyarakat berhubungan langsung dengan kecepatan. Korban yang melapor setelah dana berpindah berulang kali akan menghadapi peluang pemulihan yang lebih rendah. Faktor kebudayaan menuntut perubahan perilaku. Penggunaan kata sandi yang sama, pemberian kode autentikasi, dan peminjaman rekening kepada orang lain membentuk kondisi yang memudahkan penipuan.

C. Faktor Penghambat Penegakan Hukum

1. Faktor Internal

Hambatan internal pertama ialah keterbatasan sumber daya manusia yang memiliki kompetensi hukum dan teknis secara seimbang. Penyidikan siber membutuhkan kemampuan membaca log, melakukan akuisisi data, menilai konfigurasi akun, dan memahami jaringan. Kompetensi ini harus disertai pemahaman tentang izin penggeledahan, penyitaan, autentikasi, hak korban, dan batas privasi. Kekurangan pada salah satu sisi dapat membuat bukti yang secara teknis berguna kehilangan nilai hukum.

Hambatan kedua ialah keterbatasan alat *digital forensic*. Perangkat lunak forensik memerlukan lisensi, pembaruan, dan validasi. Perangkat terbaru memakai enkripsi, pengamanan biometrik, dan penyimpanan berbasis cloud. Tidak semua data tersimpan dalam perangkat. Sebagian informasi harus diminta kepada penyedia layanan. Ketergantungan pada satu alat juga berisiko karena hasil pemeriksaan perlu diuji dengan metode lain atau dijelaskan oleh ahli.

Hambatan ketiga ialah pengelolaan bukti elektronik. Data digital mudah disalin, tetapi kemudahan menyalin tidak sama dengan kemudahan membuktikan keaslian. Penyidik harus mencatat sumber, metode akuisisi, nilai hash, waktu, petugas, dan setiap perpindahan. KUHAP baru menyatakan bahwa alat bukti harus dapat diautentikasi dan diperoleh secara tidak melawan hukum. Apabila izin penggeledahan atau penyitaan ditolak, hasilnya dapat tidak digunakan sebagai alat bukti. Ketentuan ini menuntut administrasi yang tertib sejak awal.

Hambatan keempat ialah koordinasi yang berlapis. Data dapat berada pada bank, penyedia uang elektronik, operator telekomunikasi, *platform* media sosial, dan penyedia layanan luar negeri. Setiap lembaga memiliki prosedur, standar permintaan, dan waktu respons. Keterlambatan satu pihak dapat membuat log berakhir masa simpan atau dana berpindah. Karena itu, penyidik membutuhkan kontak kelembagaan, format permintaan yang baku, dan mekanisme respons cepat.

2. Faktor Eksternal

Hambatan eksternal pertama ialah penggunaan identitas palsu. Pelaku dapat memakai kartu SIM yang tidak mencerminkan pengguna, akun dengan foto curian, alamat fiktif, atau dokumen identitas milik orang lain. Identitas akun hanya merupakan titik awal. Penyidik perlu menghubungkannya dengan data perangkat, pola login, transaksi, lokasi, dan komunikasi.

Hambatan kedua ialah rekening pinjaman atau *money mule*. Pelaku dapat membeli, menyewa, atau meminjam rekening untuk menerima dana. Dana kemudian dipindahkan ke rekening lain, uang elektronik, aset digital, atau ditarik tunai. Pola ini memutus hubungan langsung antara korban dan pelaku utama. Penegakan hukum perlu membedakan pemilik rekening yang tertipu, lalai, memperoleh imbalan, atau sejak awal mengetahui tujuan penggunaan rekening.

Hambatan ketiga ialah VPN, *server* luar negeri, dan *platform* lintas yurisdiksi. VPN dapat menyamarkan alamat internet asal. Server luar negeri membuat permintaan data bergantung pada kebijakan perusahaan dan kerja sama internasional. Pasal 43 UU ITE membuka kerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti. Namun, efektivitasnya tetap dipengaruhi perjanjian, standar legal process, bahasa, retensi data, dan kecepatan respons. Fitriati et al. (2022) juga menemukan bahwa kerja sama lintas negara dan ahli telematika dibutuhkan ketika jejak teknis berada di luar kewenangan langsung penyidik.

Hambatan keempat ialah keterlambatan dan rendahnya literasi digital. Korban kadang merasa malu, berharap pelaku mengembalikan uang, atau tidak mengetahui saluran pelaporan. Sebagian korban menghapus percakapan dan memblokir akun sebelum menyimpan data. Ada pula korban yang memberikan akses jarak jauh kepada pelaku atau terus mentransfer dana karena dijanjikan pengembalian. Edukasi harus menjelaskan tindakan konkret setelah kejadian, yaitu menghentikan komunikasi, mengamankan akun,

menghubungi bank, melapor ke IASC untuk penipuan keuangan, dan membuat laporan polisi dengan bukti yang tersedia.

Hambatan kelima ialah kecepatan inovasi modus. Pelaku menggabungkan informasi terbuka, kecerdasan buatan, rekayasa suara, tautan palsu, dan teknik psikologis. Identitas yang tampak meyakinkan belum tentu autentik. Aparat perlu memperbarui pola deteksi dan materi edukasi secara berkala. Pencegahan yang hanya mengulang pesan umum untuk berhati-hati tidak cukup. Pesan harus menjelaskan indikator risiko, prosedur verifikasi, dan tindakan cepat.

D. Analisis Yuridis

1. Kesesuaian Prosedur Penyidikan dengan KUHAP dan UU ITE

KUHAP baru menempatkan penggeledahan Informasi Elektronik dan Dokumen Elektronik dalam rezim upaya paksa. Pasal 112 Undang-Undang Nomor 20 Tahun 2025 memperbolehkan penyidik melakukan penggeledahan terhadap Informasi Elektronik dan Dokumen Elektronik untuk kepentingan penyidikan. Pada prinsipnya, penyidik harus memperoleh izin ketua pengadilan negeri. Dalam keadaan mendesak, penggeledahan dapat dilakukan lebih dahulu, tetapi penyidik wajib meminta persetujuan dalam batas waktu yang ditentukan. Penolakan persetujuan membuat hasil penggeledahan tidak dapat dipakai sebagai alat bukti.

Penyitaan juga memerlukan izin pengadilan, kecuali keadaan mendesak terhadap benda bergerak dengan kewajiban meminta persetujuan kemudian. Aturan tersebut relevan terhadap telepon seluler, komputer, media penyimpanan, dan perangkat lain. Namun, penyitaan perangkat tidak selalu berarti penyidik bebas memeriksa seluruh data. Pemeriksaan harus berkaitan dengan tindak pidana yang disidik. Prinsip pembatasan tujuan perlu diterapkan untuk melindungi data pribadi yang tidak relevan.

Pasal 43 UU ITE melengkapi hukum acara umum. Penyidikan harus memperhatikan privasi, kerahasiaan, layanan publik, dan integritas data. Penyidik dapat meminta data dari Penyelenggara Sistem Elektronik serta memerintahkan pemutusan akses sementara terhadap akun, rekening bank, uang elektronik, atau aset digital. Ketentuan ini memberi dasar untuk tindakan cepat. Namun, tindakan tersebut tetap harus terdokumentasi, proporsional, dan dapat diuji. Kewenangan teknis tidak menghapus kewajiban *due process of law*.

2. Kedudukan dan Keabsahan Alat Bukti Elektronik

Pasal 5 UU ITE menyatakan Informasi Elektronik, Dokumen Elektronik, dan hasil cetaknya sebagai alat bukti hukum yang sah. KUHAP baru kemudian menegaskan bukti elektronik sebagai salah satu alat bukti dalam Pasal 235. KUHAP baru juga membuka penggunaan segala sesuatu untuk pembuktian sepanjang diperoleh secara tidak melawan hukum. Dua syarat utama berlaku. Alat bukti harus dapat diautentikasi dan harus diperoleh secara sah. Hakim berwenang menilai kedua syarat tersebut.

Autentikasi menjawab pertanyaan apakah data berasal dari sumber yang dinyatakan, utuh, dan berkaitan dengan perkara. Autentikasi tidak selalu memerlukan satu bentuk bukti. Penyidik dapat menggabungkan pemeriksaan perangkat, data akun, log, metadata, nilai hash, keterangan korban, keterangan ahli, data bank, dan data dari *platform*. Tangkapan layar tanpa data pendukung memiliki daya bukti lebih rendah daripada percakapan yang diperoleh melalui akuisisi perangkat dan dikonfirmasi oleh data penyedia layanan.

Keabsahan perolehan menjawab pertanyaan apakah penyidik memperoleh data melalui kewenangan dan prosedur yang benar. Data yang diambil dari perangkat melalui penggeledahan atau penyitaan tanpa dasar dapat ditolak. Data hasil intersepsi juga tunduk pada ketentuan khusus. Karena itu, penyidik harus menentukan sejak awal apakah data diberikan sukarela oleh korban, diminta dari pihak ketiga, diperoleh melalui penggeledahan, atau berasal dari penyitaan. Setiap jalur memiliki dasar dan dokumentasi yang berbeda.

Prinsip *chain of custody* menjaga hubungan antara barang bukti yang disita, salinan forensik, hasil analisis, dan bukti yang diajukan di pengadilan. Catatan harus menunjukkan siapa yang memegang, kapan berpindah, apa yang dilakukan, dan apakah nilai hash berubah. Kesalahan administrasi tidak selalu membuktikan data palsu, tetapi dapat melemahkan keyakinan atas integritas bukti. Oleh karena itu, formulir, ruang penyimpanan, akses terbatas, dan audit internal menjadi bagian dari perlindungan pembuktian.

3. Perlindungan Hak Korban dan Pemulihan Kerugian

Penanganan penipuan digital perlu memandang korban sebagai subjek yang memiliki hak, bukan hanya sumber keterangan. Pasal 144 KUHAP baru memberi korban hak atas informasi perkembangan perkara, pendampingan advokat, perlindungan keamanan dan

identitas, nasihat hukum, serta restitusi. Hak tersebut harus diterjemahkan ke dalam layanan yang mudah diakses. Korban perlu mengetahui nomor laporan, penyidik yang menangani, kebutuhan bukti tambahan, perkembangan pemblokiran, dan cara mengajukan restitusi.

Pemulihan dana membutuhkan tindakan cepat. Pemblokiran rekening mencegah perpindahan, sedangkan penyitaan dan restitusi memberi dasar pemulihan dalam proses pidana. Koordinasi dengan IASC, bank, dan penyedia pembayaran dapat mendukung pemblokiran awal. Namun, penyidik harus menjaga pemisahan fungsi. IASC menangani respons cepat sektor keuangan, sedangkan penetapan tanggung jawab pidana dan penyitaan berjalan menurut hukum acara. Data Otoritas Jasa Keuangan pada 2026 menunjukkan bahwa koordinasi lintas lembaga dapat menghasilkan pengembalian dana. Capaian tersebut harus diikuti prosedur yang transparan agar korban memahami status dan sumber pengembalian.

Perlindungan korban juga mencakup keamanan digital setelah kejadian. Pelaku mungkin masih menguasai akun, data pribadi, atau akses perangkat. Petugas perlu memberi arahan untuk mengganti kata sandi, mencabut sesi login, memulihkan akun, memblokir kartu dan rekening bila diperlukan, serta menyimpan bukti sebelum perubahan dilakukan. Pendekatan ini mengurangi kerugian lanjutan dan menjaga kualitas bukti.

4. Pertanggungjawaban Pidana Pelaku dan Hubungan Antar-Ketentuan

Analisis pertanggungjawaban dimulai dari perbuatan nyata setiap pihak. Pelaku yang membuat rangkaian kebohongan dan mengarahkan korban mentransfer dana dapat bertanggung jawab atas penipuan. Pelaku yang mengambil alih akun dapat bertanggung jawab atas akses tanpa hak. Pihak yang memanipulasi identitas atau informasi agar tampak autentik dapat bertanggung jawab atas manipulasi Informasi Elektronik. Pihak yang menampung dan memindahkan dana dapat dimintai pertanggungjawaban apabila mengetahui tujuan tindak pidana atau terbukti membantu pelaksanaan dan penyamaran hasil kejahatan.

Hubungan Pasal 492 KUHP dengan Pasal 28 ayat (1) UU ITE tidak boleh diselesaikan hanya dengan anggapan bahwa UU ITE selalu merupakan *lex specialis* karena media yang digunakan adalah internet. Kekhususan Pasal 28 ayat (1) berasal dari unsur pemberitahuan bohong atau informasi menyesatkan, kerugian materiel, konsumen,

dan Transaksi Elektronik. Apabila unsur tersebut terpenuhi, pasal UU ITE memiliki relevansi khusus. Apabila unsur konsumen atau transaksi elektronik tidak terpenuhi, Pasal 492 KUHP tetap menjadi dasar utama. Penilaian harus dilakukan terhadap fakta konkret.

Penerapan beberapa pasal dimungkinkan ketika perbuatan memiliki objek dan akibat yang berbeda. Pengambilalihan akun dapat selesai sebelum penipuan terhadap pengikut dilakukan. Manipulasi data dapat menjadi sarana terpisah untuk membuat akun tampak autentik. Namun, penyidik dan penuntut umum harus menghindari duplikasi yang menghukum perbuatan yang sama secara tidak proporsional. KUHP baru menyediakan aturan perbarengan yang perlu dipakai untuk menentukan bentuk dakwaan dan pidana secara tepat.

Dari perspektif efektivitas, kerangka hukum saat ini lebih kuat dibanding kerangka sebelum 2026. KUHP memberi rumusan penipuan nasional. KUHAP mengakui bukti elektronik serta memperkuat hak korban. UU ITE memberi kewenangan teknis dan delik khusus. UU Penyesuaian Pidana menyelaraskan ancaman denda. Kelemahan utama tidak hanya berada pada kekurangan norma, tetapi pada kecepatan pelaporan, kualitas autentikasi, akses lintas lembaga, kapasitas forensik, dan kemampuan memulihkan aset.

5. Perbandingan Norma, Teori, dan Praktik

Secara normatif, hukum telah menyediakan unsur delik, alat bukti, kewenangan penyidik, upaya paksa, dan hak korban. Menurut teori Soerjono Soekanto, norma tersebut hanya menjadi satu faktor. Praktik Polda Kalimantan Timur menunjukkan bahwa pelaku memanfaatkan media sosial, penyamaran, data calon pembeli, dan transaksi bank. Praktik tersebut menuntut aparat yang mampu menghubungkan bukti komunikasi dengan identitas pelaku dan aliran dana. Dengan demikian, titik kritis penegakan hukum berada pada hubungan antara faktor hukum, aparat, dan sarana.

Faktor masyarakat dan kebudayaan juga berpengaruh. Korban yang segera melapor memberi peluang lebih besar bagi pemblokiran. Masyarakat yang tidak membagikan kode autentikasi mengurangi risiko pengambilalihan akun. Pemilik rekening yang menolak meminjamkan rekening mengurangi jaringan penampung dana. Karena itu, strategi penegakan hukum perlu menggabungkan tindakan represif, pemulihan dana, edukasi berbasis modus, dan kewajiban kepatuhan dari penyelenggara layanan.

Berdasarkan perbandingan tersebut, praktik penyidikan dinilai sesuai dengan hukum apabila memenuhi empat standar. Pertama, kualifikasi pasal mengikuti unsur yang

terbukti. Kedua, penggeledahan, penyitaan, dan permintaan data memiliki dasar yang sah. Ketiga, bukti elektronik diautentikasi melalui prosedur yang dapat diuji. Keempat, korban memperoleh informasi, perlindungan, dan akses pemulihan. Penyidikan yang berhasil menangkap pelaku tetapi mengabaikan legalitas bukti atau hak korban belum memenuhi ukuran penegakan hukum yang utuh.

KESIMPULAN DAN SARAN

Penyalahgunaan media elektronik dalam tindak pidana penipuan muncul melalui penawaran jual beli palsu, penyamaran identitas, *phishing*, investasi bodong, *love scam*, pengambilalihan akun, dan manipulasi informasi. Media elektronik dapat menjadi sarana, objek serangan, tempat bukti tersimpan, dan jalur pemindahan hasil kejahatan. Karena bentuk perbuatannya berbeda, penipuan melalui internet tidak dapat dikualifikasikan dengan satu pasal secara otomatis.

Pasal 492 KUHP menjadi dasar penipuan umum ketika tipu muslihat atau rangkaian kebohongan menggerakkan korban menyerahkan harta. Pasal 28 ayat (1) UU ITE berlaku lebih khusus apabila informasi elektronik yang bohong atau menyesatkan menimbulkan kerugian materiel bagi konsumen dalam Transaksi Elektronik. Akses tanpa hak dan manipulasi data harus dinilai dengan ketentuan UU ITE yang sesuai. Setelah penyesuaian pada 2026, ancaman Pasal 45A ayat (1) ialah penjara paling lama enam tahun dan/atau denda kategori V sebesar Rp500.000.000,00.

Penegakan hukum oleh Unit Cyber perlu melalui penerimaan laporan, penyelidikan, penyidikan, pemeriksaan *digital forensic*, pelacakan rekening dan data akun, penetapan tersangka, serta pelimpahan perkara. KUHAP baru mengakui bukti elektronik secara tegas, tetapi bukti harus autentik dan diperoleh secara sah. Hambatan utama terdiri atas keterbatasan sumber daya dan alat, pengelolaan *chain of custody*, identitas palsu, rekening penampung, VPN, *server* luar negeri, keterlambatan laporan, dan rendahnya literasi digital. Efektivitas penegakan hukum bergantung pada keselarasan norma, kompetensi aparat, sarana, partisipasi masyarakat, dan budaya keamanan digital.

Kerangka hukum yang berlaku telah memberi dasar yang memadai, tetapi implementasinya perlu memperkuat kecepatan pemblokiran, koordinasi lintas lembaga, autentikasi bukti, dan perlindungan korban. Penanganan perkara harus mengejar dua hasil sekaligus, yaitu pertanggungjawaban pidana pelaku dan pemulihan kerugian korban.

Saran

Polda Kalimantan Timur perlu menyusun pedoman internal untuk membedakan penerapan Pasal 492 KUHP, Pasal 28 ayat (1) UU ITE, serta ketentuan akses dan manipulasi data. Pedoman perlu memuat daftar bukti minimum berdasarkan modus dan standar dokumentasi *digital forensic*.

Unit Cyber perlu memperkuat pelatihan penyidik, peralatan forensik, penyimpanan barang bukti, dan sistem *chain of custody*. Koordinasi dengan bank, IASC, operator telekomunikasi, *platform*, kejaksaan, dan penyidik wilayah lain perlu memakai jalur cepat serta format permintaan data yang baku.

Korban perlu memperoleh panduan singkat tentang penyimpanan bukti, pengamanan akun, pelaporan kepada bank dan IASC, pembuatan laporan polisi, serta pengajuan restitusi. Edukasi publik harus memakai contoh modus yang aktual dan menjelaskan tindakan yang harus dilakukan dalam jam-jam pertama setelah kejadian.

Penelitian lanjutan perlu melakukan wawancara dengan penyidik Unit Cyber Polda Kalimantan Timur dan menelaah berkas perkara yang telah berkekuatan hukum tetap. Data tersebut diperlukan untuk mengukur waktu penanganan, keberhasilan pelacakan pelaku, jumlah rekening yang diblokir, pemulihan aset, dan hambatan kerja sama dengan penyedia layanan.

DAFTAR PUSTAKA

Almas, Z. P., Novika, T., Anisa, & Glory, N. C. (2024). Analisis yuridis terkait tindak pidana penipuan online shop ditinjau menurut UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. De Juncto Delicti: Journal of Law, 4(2), 57–67. https://doi.org/10.35706/djd.v4i2.7963

Dewi, N. M. T., & Fahrial, R. L. (2022). Suatu kajian yuridis terhadap penggunaan alat bukti elektronik dalam kejahatan cyber dalam sistem penegakan hukum. Jurnal Hukum Saraswati, 3(2). https://doi.org/10.36733/jhshs.v3i2.2949

Fitriati, Faniyah, I., & Rahmad, N. (2022). Hambatan teknis penyidikan tindak pidana manipulasi informasi elektronik pada Polda Sumatera Barat. Masalah-Masalah Hukum, 51(4), 390–400. https://doi.org/10.14710/mmh.51.4.2022.390-400

Indonesia. (2023). Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023

Indonesia. (2024). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024

Indonesia. (2025). Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana. https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025

Indonesia. (2026). Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana. https://peraturan.bpk.go.id/Details/337869/uu-no-1-tahun-2026

Kifli, S. (2025). Penegakan hukum pidana di Indonesia terhadap pengaruh negatif perkembangan cyber crime. The Juris, 9(1), 182–188. https://doi.org/10.56301/juris.v9i1.1561

Otoritas Jasa Keuangan. (2025, 28 Maret). Waspada penipuan website mengatasnamakan Indonesia Anti-Scam Centre (IASC). https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/Waspada-Penipuan-Website-Mengatasnamakan-Indonesia-Anti-Scam-Centre-IASC.aspx

Otoritas Jasa Keuangan. (2026, 21 Januari). Indonesia Anti-Scam Centre berhasil kembalikan Rp161 miliar dana masyarakat korban scam. https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/IASC-Berhasil-Kembalikan-Rp161-Miliar-Dana-Masyarakat-Korban-Scam.aspx

Polda Kalimantan Timur. (2024, 31 Januari). Gelar konferensi pers, Ditreskrimsus Polda Kaltim ungkap kasus tindak pidana UU ITE. https://tribratanews.kaltim.polri.go.id/gelar-konferensi-pers-ditreskrimsus-polda-kaltim-ungkap-kasus-tindak-pidana-uu-ite/

Polda Kalimantan Timur. (2025, 12 April). Melalui talkshow “Ngopi” dengan BTV, Polda Kaltim ingatkan masyarakat untuk waspada terhadap penipuan online. https://tribratanews.kaltim.polri.go.id/melalui-talkshow-ngopi-dengan-btv-polda-kaltim-ingatkan-masyarakat-untuk-waspada-terhadap-penipuan-online/

Rahmawati, T., Takariawan, H. A., & Ramadhani, R. H. (2022). Penegakan hukum tindak pidana penipuan berbasis online dengan modus giveaway di platform media sosial. Paulus Law Journal, 3(2), 102–118. https://doi.org/10.51342/plj.v3i2.363

Reinaldo, M. K., Mahmud, H., & Faried, F. S. (2023). Tinjauan yuridis tentang penipuan penjualan smartphone melalui media belanja online OLX. Jurnal Bevinding, 1(5), 43–48.

Sanjaya, A. A., Hartono, M. S., & Ardhya, S. N. (2022). Penggunaan akun media sosial sebagai alat bukti elektronik dalam proses penyidikan. Jurnal Komunitas Yustisia, 5(2), 482–499. https://doi.org/10.23887/jatayu.v5i2.51665

Soekanto, S. (2019). Faktor-faktor yang mempengaruhi penegakan hukum (Cetakan ke-16). Rajawali Pers.

Zahrulswendar, I. H., Amrianto, A. D., & Ansori, M. A. (2021). Penegakan hukum tindak pidana penipuan melalui sarana panggilan suara dari telepon seluler. Indonesian Journal of Criminal Law and Criminology, 2(3), 147–159. https://doi.org/10.18196/ijclc.v2i3.12351