Volume 4 Number 1 (2026)
January – June 2026
Page: 55-66

Journal of Creative Power and Ambition (JCPA)
https://edujavare.com/index.php/jcpa
E-ISSN: 3031-4054
DOI: 10.70610/jcpa.1392

Analisis Yuridis Terhadap Tindak Pidana Penipuan Berbasis Digital di Indonesia

Yoga Dwi Utama[1], Muhammad Zainuddin[2], Idul Hamzah Alid[3]

Universitas Darul Ulum Islamic Centre Sudirman
*Coresponding Email: yogadwiutama15@gmail.com

Article history Submitted: 2026/02/01; Revised: 2026/03/11; Accepted: 2026/06/11

Abstract

The rapid advancement of digital technology has created new avenues for fraudulent conduct that far exceeds the reach of conventional criminal law. Digital-based fraud encompassing phishing, social engineering, online shopping scams, and fraudulent investment schemes disguised as digital platforms shows a consistently rising trend and inflicts enormous financial losses on Indonesian society. This study examines how Indonesian criminal law constructs liability for digital fraud, particularly through the Criminal Code (KUHP), Law Number 11 of 2008 as amended by Law Number 19 of 2016 on Electronic Information and Transactions (UU ITE), and Law Number 8 of 1999 on Consumer Protection. A normative juridical method is employed, using statutory and conceptual approaches. The analysis reveals that conventional fraud provisions in the Criminal Code are insufficient to capture the unique characteristics of digital fraud, while UU ITE offers more relevant penal provisions yet leaves interpretive uncertainties regarding key elements of the offense. Key challenges identified include difficulties in proving elements of deception and criminal intent in digital contexts, perpetrator anonymity, and insufficient inter-agency coordination in handling cross-border cases. The study recommends strengthened digital investigative capacity, uniform juridical interpretation of digital fraud offense elements, and enhanced technical implementation regulations.

Keywords Digital Fraud; Cybercrime; UU ITE; Criminal Liability; Indonesian Criminal Law

INTRODUCTION

Kemajuan teknologi digital yang berlangsung dengan cepat dalam dua dekade terakhir telah mengubah hampir seluruh sendi kehidupan manusia, termasuk cara orang bertransaksi, berkomunikasi, dan mencari informasi. Namun di balik segala kemudahan yang ditawarkan, digitalisasi juga membuka ruang-ruang baru bagi kejahatan yang tidak dikenal sebelumnya atau lebih tepatnya, memberikan wajah baru pada kejahatan lama. Penipuan, yang dalam sejarah hukum pidana selalu ada

dalam satu bentuk atau lainnya, kini hadir dalam rupa yang jauh lebih canggih: berkedok toko daring palsu, menggunakan akun media sosial tiruan tokoh terkenal, memanfaatkan rasa panik korban melalui pesan singkat darurat, atau menyamar sebagai platform investasi yang menjanjikan keuntungan tidak masuk akal. Data dari Badan Reserse Kriminal Polri menunjukkan bahwa laporan kasus penipuan berbasis digital terus meningkat setiap tahunnya. Pada 2023, kejahatan siber secara keseluruhan yang dilaporkan ke kepolisian mencapai lebih dari 11.800 kasus, dengan penipuan dan penipuan online menempati porsi terbesar. Angka ini pun masih diyakini merupakan gunung es, jauh di bawah jumlah kejadian sesungguhnya, karena banyak korban yang memilih tidak melapor karena malu, tidak tahu caranya, atau pesimis kasusnya akan ditindaklanjuti. Nilai kerugian yang diakibatkan pun tidak kecil: Otoritas Jasa Keuangan (OJK) memperkirakan kerugian akibat penipuan digital di sektor keuangan saja mencapai ratusan miliar rupiah per tahun. Di sisi regulasi, Indonesia sebenarnya sudah memiliki beberapa instrumen hukum yang relevan. Pasal 378 KUHP tentang penipuan merupakan norma pokok yang paling sering digunakan, namun rumusannya yang berorientasi pada interaksi tatap muka membuatnya tidak selalu tepat untuk menjangkau modus-modus penipuan yang sepenuhnya berlangsung di ruang digital. UU ITE hadir mengisi sebagian celah itu Pasal 28 ayat (1) misalnya mengatur tentang berita bohong dan penyesatan yang menimbulkan kerugian konsumen dalam transaksi elektronik namun implementasinya di lapangan masih tidak seragam dan menimbulkan banyak perdebatan tentang tafsir unsur-unsurnya.

Penipuan dalam hukum pidana Indonesia diatur secara pokok dalam Pasal 378 KUHP yang merumuskan: barangsiapa 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 utang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun. Ada beberapa unsur kunci dalam rumusan Pasal 378 KUHP yang perlu dipahami dengan baik. Pertama, unsur menggerakkan orang lain untuk menyerahkan sesuatu ini mensyaratkan adanya hubungan kausal antara cara-cara yang digunakan pelaku (nama palsu, tipu muslihat, rangkaian kebohongan) dengan tindakan korban yang kemudian menyerahkan sesuatu. Kedua, unsur maksud menguntungkan diri sendiri atau orang lain secara melawan hukum ini adalah elemen kesengajaan (dolus specialis) yang harus dibuktikan. Ketiga, unsur tipu muslihat atau rangkaian kebohongan

yang dalam konteks digital menjadi sangat elastis dan memerlukan penafsiran yang lebih kontekstual. Persoalan yang muncul ketika Pasal 378 KUHP diterapkan pada kasus penipuan digital adalah bahwa rumusannya mengandaikan interaksi yang bersifat langsung dan personal antara pelaku dan korban. Konsep 'menggerakkan' seseorang untuk menyerahkan sesuatu secara tradisional dibayangkan sebagai tindakan persuasi yang terjadi dalam konteks tatap muka atau setidaknya komunikasi yang relatif langsung. Dalam penipuan digital, pelaku bisa berinteraksi dengan ribuan korban potensial secara serentak melalui pesan massal, iklan palsu, atau antarmuka aplikasi yang dirancang untuk menipu tanpa pernah melakukan kontak personal dengan satupun dari mereka.

Untuk mengisi keterbatasan KUHP, UU ITE mengatur beberapa ketentuan yang lebih relevan dengan konteks digital. 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 diancam pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp 1 miliar berdasarkan Pasal 45A. Selain itu, Pasal 35 UU ITE mengatur tentang manipulasi informasi elektronik—yang relevan untuk kasus di mana pelaku memanipulasi antarmuka atau dokumen digital untuk menciptakan kesan palsu. Di tingkat perlindungan konsumen, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen juga memberikan instrumen yang relevan, terutama Pasal 8 tentang larangan pelaku usaha memperdagangkan barang atau jasa yang tidak sesuai dengan yang diperjanjikan, dan Pasal 62 yang mengancam pidana penjara hingga 5 tahun dan/atau denda hingga Rp 2 miliar. Meskipun UUPK bukan regulasi pidana khusus, ketentuan pidananya dapat menjadi dasar penuntutan tambahan dalam kasus penipuan belanja daring yang melibatkan pelaku usaha.

Tabel 1. Perbandingan Regulasi Penipuan Digital di Indonesia

Aspek	KUHP Pasal 378	UU ITE Pasal 28 jo. 45A	UUPK Pasal 8 jo. 62
Ancaman pidana	Maks. 4 tahun penjara	Maks. 6 tahun penjara / denda Rp 1 M	Maks. 5 tahun / denda Rp 2 M
Unsur utama	Tipu muslihat / kebohongan + menggerakkan orang menyerahkan sesuatu	Berita bohong dan menyesatkan + kerugian konsumen transaksi elektronik	Barang/jasa tidak sesuai perjanjian dalam hubungan pelaku usaha-konsumen
Medium	Tidak terbatas (termasuk digital)	Khusus medium elektronik	Perdagangan barang/jasa (online maupun offline)
Subjek pelaku	Siapapun	Siapapun	Pelaku usaha

Pembuktian mens rea	Kesengajaan + niat menguntungkan diri	Kesengajaan + tanpa hak	Pelanggaran kewajiban pelaku usaha

Sumber: KUHP, UU No. 11/2008 jo. UU No. 19/2016, UU No. 8/1999

Sebelum masuk ke analisis yuridis, penting untuk memahami terlebih dahulu pola-pola penipuan digital yang paling umum terjadi di Indonesia, karena setiap modus memiliki karakteristik teknis dan yuridis yang berbeda dan menuntut pendekatan pembuktian yang berbeda pula. Phishing adalah teknik penipuan di mana pelaku membuat situs web, surel, atau pesan yang menyerupai entitas terpercaya seperti bank, marketplace, instansi pemerintah untuk mengelabui korban agar menyerahkan data sensitif seperti kata sandi atau nomor kartu kredit. Social engineering adalah pendekatan yang lebih personal, di mana pelaku memanipulasi psikologi korban secara langsung melalui telepon atau pesan untuk mendapatkan informasi atau transfer dana sering menggunakan skenario darurat seperti 'akun Anda diblokir' atau 'anak Anda kecelakaan'. Penipuan belanja daring melibatkan toko atau penjual fiktif di platform marketplace atau media sosial yang menerima pembayaran tanpa mengirimkan barang. Investasi bodong berbasis platform menggunakan antarmuka aplikasi yang tampak profesional untuk menjanjikan imbal hasil tidak realistis guna menarik modal dari korban yang kemudian tidak dapat ditarik kembali.

Perhatian akademis terhadap kejahatan siber dan penipuan digital di Indonesia memang sudah cukup banyak, namun kajian yang ada masih menyisakan sejumlah celah yang perlu diisi. Maskun (2013) memberikan kontribusi awal yang penting dengan memetakan jenis-jenis kejahatan siber dalam perspektif hukum pidana Indonesia secara komprehensif. Namun kajiannya bersifat sangat umum penipuan digital hanya menjadi salah satu dari banyak kategori yang dibahas tanpa pendalaman khusus dan ditulis sebelum maraknya modus penipuan baru seperti phishing berbasis rekayasa sosial yang menyasar nasabah perbankan digital maupun investasi bodong berbasis aplikasi.

Suhariyanto (2012) mengkaji tindak pidana teknologi informasi dalam perspektif sistem peradilan pidana dan memusatkan perhatian pada aspek hukum acara dan pembuktian. Kajian ini berguna untuk memahami tantangan prosedural, namun tidak menelaah secara mendalam bagaimana unsur-unsur materiil penipuan dalam KUHP berinteraksi dengan ketentuan UU ITE ketika diterapkan pada kasus penipuan digital sebuah persoalan yang sangat krusial dalam praktik penuntutan. Ramadhan (2022) meneliti pertanggungjawaban pidana pelaku penipuan online dan mengidentifikasi bahwa Pasal 28 UU ITE belum dipahami secara seragam oleh aparat penegak hukum; namun penelitiannya terbatas pada kasus penipuan belanja

daring dan tidak menjangkau modus-modus penipuan digital lain yang kini lebih dominan seperti penipuan investasi dan social engineering.

Wahyudi (2020) secara khusus mengkaji penipuan investasi bodong dalam perspektif hukum pidana ekonomi dan menemukan bahwa penegakan hukumnya sering terjebak dalam dikotomi antara hukum pidana umum dan hukum pidana khusus di bidang pasar modal. Meski sangat relevan, kajiannya tidak membahas aspek digital dari penipuan investasi padahal justru platform digital yang menjadi medium utama penipuan investasi dalam beberapa tahun terakhir. Sementara itu, Putri dan Yulianti (2023) menganalisis penggunaan Pasal 378 KUHP dalam kasus penipuan daring dan menemukan banyak putusan yang tidak konsisten, namun kajian mereka berbasis analisis putusan pengadilan yang bersifat deskriptif tanpa mengurai secara sistematis di mana letak kelemahan konstruksi unsur deliknya. Dari pemetaan tersebut, teridentifikasi tiga celah akademis yang menjadi pijakan penelitian ini. Pertama, belum ada kajian yang secara terpadu menganalisis interaksi normatif antara Pasal 378 KUHP, Pasal 28 UU ITE, dan ketentuan relevan dalam UUPK dalam menghadapi berbagai modus penipuan digital yang kini ada mulai dari phishing, social engineering, penipuan belanja daring, hingga investasi bodong berbasis platform. Kedua, perdebatan tentang unsur-unsur delik penipuan digital khususnya tentang apa yang dimaksud 'tipu muslihat' dan 'kebohongan' dalam konteks pesan teks, iklan digital, atau antarmuka aplikasi belum pernah dikaji secara sistematis dalam satu kerangka analisis yang kohesif. Ketiga, implikasi dari anonimitas dan lintas batas dalam penipuan digital terhadap konstruksi mens rea dan pembuktian belum mendapat perhatian yang proporsional dalam literatur hukum pidana Indonesia.

Penelitian ini hadir untuk menjawab ketiga celah tersebut. Yang membedakannya dari kajian-kajian sebelumnya adalah pendekatannya yang lintas-modus dan lintas-regulasi: alih-alih memfokuskan diri pada satu jenis penipuan atau satu peraturan saja, tulisan ini memetakan berbagai modus penipuan digital yang relevan, menganalisis bagaimana setiap regulasi merespons masing-masing modus tersebut, dan secara khusus membedah persoalan pembuktian unsur kesengajaan dan kebohongan yang menjadi titik paling krusial sekaligus paling sering menjadi perdebatan—dalam penuntutan kasus penipuan digital. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Bahan hukum primer meliputi KUHP, UU ITE beserta perubahannya, UUPK, dan KUHAP. Bahan hukum sekunder mencakup literatur akademik, jurnal hukum, laporan lembaga penegak

hukum dan otoritas terkait, serta putusan pengadilan yang relevan. Analisis dilakukan secara deskriptif-analitis untuk memahami konstruksi normatif delik penipuan digital sekaligus mengidentifikasi celah dan tantangan implementasinya.

METHODS

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan (statute approach) dan pendekatan kasus (case approach). Pendekatan perundang-undangan dilakukan melalui pengkajian berbagai regulasi yang mengatur tindak pidana penipuan berbasis digital di Indonesia, seperti Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, serta peraturan terkait lainnya. Sementara itu, pendekatan kasus digunakan untuk menganalisis berbagai putusan pengadilan dan praktik penegakan hukum terhadap tindak pidana penipuan yang dilakukan melalui media elektronik, platform digital, maupun sarana komunikasi berbasis internet.

Data penelitian diperoleh melalui studi kepustakaan dengan menggunakan bahan hukum primer, sekunder, dan tersier. Bahan hukum primer terdiri atas peraturan perundang-undangan, putusan pengadilan, dan dokumen resmi yang relevan. Bahan hukum sekunder meliputi buku, jurnal ilmiah, artikel hukum, serta hasil penelitian yang membahas kejahatan siber dan penipuan digital. Adapun bahan hukum tersier berupa kamus hukum, ensiklopedia, dan sumber referensi lainnya yang mendukung penelitian. Seluruh data dianalisis secara kualitatif dengan metode deskriptif-analitis, yaitu menguraikan ketentuan hukum yang berlaku, mengidentifikasi permasalahan hukum yang muncul dalam praktik, serta mengevaluasi efektivitas pengaturan dan penegakan hukum terhadap tindak pidana penipuan berbasis digital di Indonesia.

FINDINGS AND DISCUSSION

Kesesuaian Pasal 378 KUHP dengan Karakteristik Penipuan Digital

Menerapkan Pasal 378 KUHP pada kasus penipuan digital bukan perkara yang sederhana. Ada dua persoalan yuridis utama yang muncul dalam praktik. Pertama adalah persoalan tentang apakah 'tipu muslihat' dan 'rangkaian kebohongan' dalam rumusan pasal tersebut dapat mencakup bentuk-bentuk penipuan yang dilakukan melalui medium digital. Mahkamah Agung dalam beberapa putusannya telah memperluas tafsir unsur ini untuk mencakup tindakan yang dilakukan melalui pesan elektronik namun penafsiran yang konsisten belum tercipta di semua tingkat pengadilan. Persoalan kedua dan yang lebih fundamental adalah unsur

'menggerakkan orang lain untuk menyerahkan sesuatu'. Dalam penipuan digital berskala besar seperti phishing massal, pelaku tidak pernah melakukan komunikasi personal dengan setiap korban ia cukup membuat satu halaman web palsu atau mengirim satu pesan teks secara massal, lalu menunggu siapa saja yang tertipu. Apakah dalam kondisi ini masih ada 'penggerakan' dalam arti yang dimaksud Pasal 378? Sebagian akademisi berpendapat bahwa 'penggerakan' tidak mensyaratkan interaksi personal dan dapat terjadi melalui medium tidak langsung sekalipun, sementara pihak lain mempertahankan bahwa unsur ini mensyaratkan setidaknya adanya komunikasi yang terarah kepada korban tertentu.

Dalam praktik penegakan hukum, ketidakjelasan tafsir ini sering membuat penyidik dan jaksa memilih menggunakan Pasal 28 UU ITE sebagai alternatif atau tambahan dakwaan karena rumusannya lebih eksplisit menyebut kerugian dalam transaksi elektronik dan tidak memerlukan pembuktian 'penggerakan' dalam arti tradisionalnya. Namun pilihan ini pun membawa konsekuensi tersendiri: Pasal 28 UU ITE tidak mensyaratkan adanya kerugian individu yang spesifik (hanya 'kerugian konsumen' secara umum), sehingga dalam beberapa kasus justru lebih sulit untuk menunjukkan bahwa penipuan benar-benar terjadi dan bukan sekadar informasi yang menyesatkan.

Pembuktian Unsur Kesengajaan: Persoalan Mens Rea di Ruang Digital

Dari seluruh unsur tindak pidana yang harus dibuktikan dalam kasus penipuan digital, pembuktian mens rea khususnya unsur kesengajaan dan niat jahat pelaku adalah yang paling menantang sekaligus paling menentukan keberhasilan penuntutan. Kesengajaan dalam hukum pidana Indonesia dibedakan menjadi tiga gradasi: (1) sengaja sebagai tujuan (dolus directus), di mana akibat yang terjadi memang dikehendaki pelaku; (2) sengaja dengan insyaf kepastian, di mana pelaku sadar bahwa akibat tertentu pasti akan terjadi meski bukan tujuan utamanya; dan (3) sengaja dengan insyaf kemungkinan (dolus eventualis), di mana pelaku sadar akan kemungkinan terjadinya akibat namun tetap melanjutkan perbuatannya. Dalam kasus penipuan digital, penyidik harus membuktikan bahwa pelaku memang mengetahui bahwa informasi yang ia sampaikan adalah palsu atau menyesatkan dan bahwa ia menghendaki korban tertipu sehingga menyerahkan sesuatu kepadanya. Persoalannya adalah bahwa kondisi batin ini hanya dapat disimpulkan dari fakta-fakta eksternal, sementara pelaku hampir selalu berdalih bahwa ia sendiri tidak mengetahui bahwa produk atau informasi yang ia iklankan adalah palsu, atau bahwa ia hanya bertindak sebagai perantara tanpa mengetahui niat penipu yang sebenarnya. Dalam konteks investasi bodong digital misalnya, rantai pelaku bisa

sangat panjang: ada pemilik platform, ada agen pemasar, ada member yang membantu merekrut anggota baru. Di antara semua aktor ini, hanya sebagian kecil yang benar-benar tahu bahwa platform tersebut adalah skema penipuan. Selebihnya bisa saja adalah korban sekaligus pelaku. Mereka turut merekrut orang lain dengan sungguh-sungguh percaya bahwa investasi itu nyata. Memilah mana yang memiliki mens rea dan mana yang tidak adalah pekerjaan investigatif yang sangat rumit dan menuntut keahlian yang lebih dari sekadar kemampuan hukum.

Tantangan Penegakan Hukum: Dari Identifikasi hingga Penuntutan

Penanganan perkara penipuan digital menghadapi rentetan tantangan yang saling berkaitan, dari tahap pelaporan hingga vonis pengadilan. Pada tahap pelaporan, banyak korban yang tidak melapor karena merasa kerugiannya terlalu kecil untuk diproses hukum, tidak tahu ke mana harus melapor, atau pesimis kasusnya akan ditindaklanjuti. Ini menciptakan masalah underreporting yang membuat skala sebenarnya kejahatan ini tidak tercermin dalam statistik resmi. Pada tahap penyelidikan, penyidik menghadapi problem identifikasi pelaku yang beroperasi di balik lapisan anonimitas digital. Berbeda dari kejahatan konvensional di mana jejak fisik pelaku dapat ditelusuri, penipuan digital seringkali hanya meninggalkan jejak berupa alamat IP, nomor rekening, dan identitas digital yang bisa dengan mudah dipalsukan atau disamarkan. Rekening bank yang digunakan pelaku sering kali adalah rekening orang lain yang dibeli atau disewa. Fenomena yang dikenal sebagai rekening joki atau money mule sehingga penyidik perlu menelusuri rantai aliran uang yang bisa sangat panjang dan berlapis. Koordinasi antarlembaga juga menjadi tantangan yang tidak kecil. Perkara penipuan digital di sektor keuangan melibatkan setidaknya tiga instansi sekaligus: kepolisian (penyidikan), OJK (pengawasan sektor keuangan), dan PPATK (penelusuran aliran dana). Dalam praktik, koordinasi ketiganya tidak selalu berjalan mulus karena perbedaan kewenangan, prosedur, dan sistem informasi yang belum terintegrasi. Sementara itu, ketika pelaku berada di luar negeri yang semakin umum dalam kasus penipuan digital prosedur mutual legal assistance yang diperlukan bisa memakan waktu berbulan-bulan bahkan bertahun-tahun.

Tabel 2. Tantangan Penegakan Hukum Penipuan Digital dan Kebutuhan Solusinya

Tahap	Tantangan Utama	Solusi yang Dibutuhkan
Pelaporan	Underreporting karena ketidaktahuan dan pesimisme korban	Kanal pelaporan yang mudah, respons yang nyata dan cepat
Penyelidikan	Anonimitas pelaku, rekening joki, jejak digital yang mudah dihapus	Kapasitas digital forensik, akses data telekomunikasi dan

		perbankan
Pembuktian	Kesulitan membuktikan mens rea dan unsur 'tipu muslihat' pada medium digital	Pedoman pembuktian khusus kejahatan siber, standardisasi tafsir yuridis
Penuntutan	Ketidakseragaman pilihan pasal dakwaan (KUHP vs. UU ITE vs. UUPK)	Pedoman teknis Kejaksaan Agung, pelatihan jaksa bidang siber
Lintas batas	Pelaku di luar negeri, server asing, yurisdiksi tumpang tindih	Perjanjian ekstradisi, kerja sama INTERPOL dan platform digital

Sumber: Analisis penulis berdasarkan literatur dan regulasi terkait (2025)

Analisis Kasus Ilustratif: Tiga Pola Penipuan Digital yang Dominan

Untuk mendekatkan analisis yuridis dengan realitas di lapangan, berikut diuraikan tiga pola kasus penipuan digital yang paling sering ditangani aparat penegak hukum dalam beberapa tahun terakhir, beserta konstruksi juridis yang relevan. Pola Pertama: Social Engineering Berbasis Telepon. Pelaku menghubungi korban via telepon sambil berpura-pura sebagai petugas bank, operator seluler, atau pegawai instansi pemerintah. Korban diberitahu bahwa rekeningnya akan diblokir atau ada transaksi mencurigakan, lalu diminta menyebutkan kode OTP atau melakukan transfer 'untuk keamanan'. Dalam pola ini, unsur 'tipu muslihat' terpenuhi dari skenario palsu yang dibangun pelaku, dan unsur 'menggerakkan korban menyerahkan sesuatu' terpenuhi dari tindakan korban yang mentransfer dana. Mens rea relatif lebih mudah dibuktikan karena ada rekaman percakapan yang dapat dianalisis. Ketentuan yang relevan: Pasal 378 KUHP dan/atau Pasal 28 ayat (1) UU ITE.

Pola Kedua: Toko Daring Fiktif di Media Sosial. Pelaku membuat akun toko di media sosial atau marketplace, mengunggah foto produk yang menarik (sering dicuri dari sumber lain), menerima pembayaran di muka, lalu menghilang tanpa mengirimkan barang. Konstruksi pidananya dapat menggunakan Pasal 378 KUHP (jika dibuktikan ada kesengajaan tidak memenuhi perjanjian sejak awal), Pasal 28 UU ITE (berita bohong dalam transaksi elektronik), maupun Pasal 62 UUPK (pelanggaran kewajiban pelaku usaha). Tantangan terbesar adalah membuktikan niat jahat sejak awal apakah ini penipuan terencana atau penjual yang genuinely gagal memenuhi pesanan karena masalah usaha. Pola Ketiga: Platform Investasi Bodong. Ini adalah pola yang menghasilkan kerugian terbesar secara agregat. Pelaku mendirikan platform atau aplikasi investasi yang tampak profesional, memberikan keuntungan nyata di awal untuk membangun kepercayaan, lalu menghilang setelah mengumpulkan dana dalam jumlah besar (skema ponzi digital). Regulasi yang berlaku bisa sangat kompleks selain KUHP dan UU ITE, kasus semacam ini bisa juga

dijerat dengan Undang-Undang Pasar Modal (jika platform menawarkan efek tanpa izin), Undang-Undang Perdagangan Berjangka Komoditi, atau Undang-Undang Tindak Pidana Pencucian Uang mengingat besarnya aliran dana yang terlibat.

Kebutuhan Mendesak: Penguatan Regulasi dan Kapasitas Penegakan

Dari seluruh analisis di atas, terlihat jelas bahwa persoalan penipuan digital di Indonesia bukan semata-mata masalah regulasi kerangka hukum yang ada sudah cukup untuk menjadi dasar penuntutan melainkan masalah tafsir, kapasitas, dan koordinasi. Ada tiga hal yang paling mendesak untuk segera dibenahi. Pertama, perlu ada penyeragaman tafsir yuridis tentang unsur-unsur delik penipuan digital. Mahkamah Agung dapat memainkan peran penting di sini melalui penerbitan SEMA (Surat Edaran Mahkamah Agung) atau peraturan mahkamah agung yang memberikan pedoman interpretasi tentang bagaimana unsur 'tipu muslihat', 'rangkaian kebohongan', dan 'menggerakkan' dalam Pasal 378 KUHP dibaca dalam konteks digital; serta bagaimana hubungan antara Pasal 378 KUHP dan Pasal 28 UU ITE ditentukan dalam dakwaan. Kedua, kapasitas teknis penyidik dan jaksa dalam menangani kejahatan digital perlu ditingkatkan secara sistematis. Ini mencakup pelatihan digital forensik, kemampuan analisis aliran dana digital, dan pemahaman tentang cara kerja berbagai platform digital yang sering menjadi medium penipuan. Tanpa kapasitas teknis yang memadai, regulasi sebagus apapun tidak akan efektif dalam menjeratkan pelaku. Ketiga, mekanisme kerja sama antara kepolisian, OJK, PPATK, dan platform digital perlu diintegrasikan secara lebih sistematis termasuk dengan platform media sosial dan marketplace yang sering menjadi arena penipuan. Kewajiban platform untuk melaporkan aktivitas mencurigakan dan kooperatif dalam penyidikan perlu diperkuat, baik melalui regulasi maupun melalui perjanjian kerja sama yang mengikat.

CONCLUSION

Tindak pidana penipuan berbasis digital adalah fenomena yang nyata, terus berkembang, dan menimbulkan kerugian besar bagi masyarakat Indonesia. Secara yuridis, kerangka hukum yang tersedia Pasal 378 KUHP, Pasal 28 UU ITE, dan ketentuan UUPK sudah memberikan dasar normatif untuk memproses pelaku, namun masing-masing mengandung kelemahan dan celah ketika dihadapkan pada karakteristik unik penipuan digital. Pasal 378 KUHP sebagai norma pokok penipuan menghadapi tantangan tafsir yang serius karena rumusannya berorientasi pada interaksi tatap muka dan tidak secara eksplisit mengakomodasi penipuan yang dilakukan melalui antarmuka digital atau komunikasi massal yang tidak personal. Pasal 28 UU ITE lebih relevan secara kontekstual namun rumusannya yang berfokus

pada 'berita bohong' dan 'kerugian konsumen' tidak sepenuhnya mencakup semua pola penipuan digital yang ada. Kombinasi dakwaan menggunakan kedua regulasi sekaligus adalah praktik yang sudah berjalan, namun belum ada panduan yang seragam tentang bagaimana memilih dan mengkombinasikannya. Pembuktian mens rea dan unsur-unsur materiil penipuan tetap menjadi tantangan terbesar. Anonimitas digital, panjangnya rantai pelaku dalam penipuan berskala besar, dan lambatnya kerja sama dengan platform digital asing menjadi variabel yang secara konsisten mempersulit penegakan hukum. Penguatan kapasitas teknis penyidik dan penyeragaman tafsir yuridis melalui pedoman Mahkamah Agung atau Kejaksaan Agung adalah dua langkah yang paling mendesak untuk meningkatkan efektivitas penanganan perkara.

REFERENCES

Ali, M. (2015). Hukum pidana Indonesia: Perkembangan dan pembaharuan. Sinar Grafika.

Arief, B. N. (2016). Bunga rampai kebijakan hukum pidana: Perkembangan penyusunan konsep KUHP baru (Cet. ke-5). Kencana Prenada Media.

Chazawi, A. (2002). Pelajaran hukum pidana bagian 1: Stelsel pidana, tindak pidana, teori-teori pemidanaan, dan batas berlakunya hukum pidana. PT RajaGrafindo Persada.

Hamzah, A. (2010). Asas-asas hukum pidana (Ed. revisi). Rineka Cipta.

Marzuki, P. M. (2016). Penelitian hukum (Ed. revisi). Kencana Prenada Media.

Maskun. (2013). Kejahatan siber (cybercrime): Suatu pengantar. Kencana Prenada Media.

Moeljatno. (2008). Asas-asas hukum pidana (Ed. ke-8). Rineka Cipta.

Prodjodikoro, W. (2003). Tindak-tindak pidana tertentu di Indonesia (Ed. ke-3). Refika Aditama.

Saleh, R. (1983). Perbuatan pidana dan pertanggungjawaban pidana: Dua pengertian dasar dalam hukum pidana. Aksara Baru.

Soekanto, S. (2012). Faktor-faktor yang memengaruhi penegakan hukum (Ed. ke-11). PT Raja Grafindo Persada.

Suhariyanto, B. (2012). Tindak pidana teknologi informasi (cybercrime): Urgensi pengaturan dan celah hukumnya. PT RajaGrafindo Persada.

Ariyanti, V. (2019). Kebijakan penegakan hukum dalam sistem peradilan pidana Indonesia. Jurnal Yuridis, 6(2), 33–54.

Farida, U. (2021). Pertanggungjawaban pidana pelaku penipuan online di Indonesia: Analisis putusan pengadilan. Jurnal Hukum Ius Quia Iustum, 28(2), 339–360.

Nugroho, C. A. (2020). Penerapan Pasal 378 KUHP dalam penanganan tindak pidana penipuan melalui media elektronik. Jurnal Hukum dan Peradilan, 9(3), 411–430.

Prasetyo, H. (2022). Problematika penerapan Pasal 28 ayat (1) UU ITE dalam kasus penipuan

transaksi elektronik. Jurnal Penelitian Hukum De Jure, 22(2), 211–228.

Putri, M. A., & Yulianti, R. (2023). Inkonsistensi putusan pengadilan dalam perkara penipuan daring: Studi terhadap penerapan Pasal 378 KUHP. Jurnal Ilmu Hukum, 19(1), 67–86.

Ramadhan, A. F. (2022). Pertanggungjawaban pidana pelaku penipuan online dalam perspektif UU ITE. Jurnal Penelitian Hukum De Jure, 22(1), 87–104.

Setiawan, D. (2021). Tantangan penegakan hukum pidana di era transformasi digital: Analisis kritis terhadap UU ITE. Masalah-Masalah Hukum, 50(2), 157–174.

Wahyudi, M. (2020). Penipuan investasi bodong dalam perspektif hukum pidana ekonomi Indonesia. Padjadjaran Jurnal Ilmu Hukum, 7(2), 195–214.

Wibowo, A. (2021). Urgensi pembaruan regulasi penipuan digital dalam merespons perkembangan modus kejahatan siber. Jurnal Hukum IUS QUIA IUSTUM, 28(3), 509–530.

Kitab Undang-Undang Hukum Pidana (Wetboek van Strafrecht).

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana. Lembaran Negara Republik Indonesia Tahun 1981 Nomor 76.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.

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

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1.

Badan Reserse Kriminal Polri. (2023). Data kejahatan siber 2023. Bareskrim Polri.

Otoritas Jasa Keuangan. (2024). Laporan tahunan pengawasan sektor jasa keuangan 2023. OJK.

Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK). (2023). Laporan tahunan PPATK 2022: Tipologi tindak pidana pencucian uang berbasis digital. PPATK.