ISSN: 2338 4638

Volume 7 Nomor 7 (2023)

'ADALAH

Buletin Hukum & Keadilan

# Anatomi Penipuan Digital dan Tantangan Penegakan Hukumnya di Indonesia: Dari *Social Engineering* hingga *Deepfake*, serta Problematika Rezim Pembuktian

**Gilang Rizki Aji Putra***

Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v7i7.51839

**Abstract:**

Digital fraud has become the most pervasive criminal modality in the digital economy, transcending territorial boundaries and systematically exploiting human psychological vulnerabilities. This article analyzes the anatomy and evolving modus operandi of digital fraud in Indonesia and identifies the multidimensional challenges in its enforcement. Using normative legal research with case, statutory, and comparative approaches, the study finds that digital fraud has evolved from conventional phishing into complex psychological manipulation schemes enhanced by deepfake technology and automated systems. The analysis reveals that Indonesia's criminal law framework, including the Penal Code and the Electronic Information and Transactions Law, still contains fundamental weaknesses in jurisdiction, evidentiary standards, and digital asset tracing. Major cases, such as binary options scams and banking social engineering schemes, confirm that law enforcement agencies often struggle to match the speed and sophistication of offenders. The article concludes that effective enforcement requires jurisdictional reform, strengthened digital forensic capacity, and enhanced international cooperation mechanisms.

**Keywords:** Digital Fraud, Social Engineering, Deepfake, Electronic Information and Transactions Law (ITE Law), Digital Evidence

* Peneliti pada Pusat Studi Konstitusi dan legislasi Nasional (Poskolegnas), Universitas Islam Negeri Syarif Hidayatullah Jakarta. Email: gilang.rizkiajiputra19@uinjkt.ac.id.

## A. PENDAHULUAN

Penipuan adalah bentuk kejahatan tertua dalam peradaban manusia. Namun, digitalisasi telah memberinya sayap baru yang membuatnya terbang lebih cepat, lebih jauh, dan lebih mematikan. Jika dulu penipu harus bertatap muka dengan korbannya, kini mereka cukup duduk di depan layar, menebar ribuan kail secara otomatis menggunakan bot, menunggu satu-dua korban yang lengah. Penipuan digital bukan lagi kejahatan sederhana; ia telah menjadi industri terorganisasi yang dijalankan oleh sindikat lintas negara, dilengkapi dengan perangkat lunak canggih, pusat panggilan palsu, dan jaringan pencucian uang digital yang rumit.

Di Indonesia, data dari Kepolisian Republik Indonesia dan Otoritas Jasa Keuangan menunjukkan bahwa penipuan digital adalah jenis kejahatan siber dengan volume laporan tertinggi. Kerugian finansial yang ditimbulkan mencapai triliunan rupiah setiap tahunnya, dan angka tersebut kemungkinan besar hanyalah puncak gunung es karena banyak korban yang enggan melapor (Bareskrim Polri, 2023). Modus yang awalnya hanya berupa *surel phishing* kini telah berevolusi menjadi *smishing*, *vishing*, *social engineering* terstruktur, hingga penggunaan deepfake untuk meniru wajah dan suara orang yang dipercaya korban.

Paradoksnya, di saat modus penipuan semakin kompleks, kerangka hukum pidana di Indonesia masih bertumpu pada instrumen yang dirancang untuk era pra-digital. Pasal 378 KUHP tentang penipuan memerlukan adanya "tipu muslihat" yang menggerakkan korban untuk menyerahkan sesuatu secara sukarela. Ketentuan ini, jika diterapkan pada penipuan digital yang serba otomatis dan melibatkan artificial intelligence, menimbulkan persoalan yuridis yang serius: apakah algoritma yang menipu memenuhi unsur "tipu muslihat"? Bagaimana membuktikan "kesukarelaan" penyerahan dalam transaksi elektronik yang terjadi dalam hitungan detik? UU ITE memang menyediakan beberapa pasal yang dapat digunakan, seperti Pasal 28 ayat (1) tentang berita bohong dan Pasal 35 tentang manipulasi data, tetapi konstruksi deliknya tidak secara spesifik dirancang untuk mengkriminalisasi penipuan digital secara komprehensif (Nugroho, 2024). Rumusan masalah dalam artikel ini adalah: Pertama, bagaimana karakteristik dan modus operandi penipuan digital yang berkembang di Indonesia? Kedua, apa tantangan utama dalam penegakan hukum terhadap penipuan digital dan bagaimana strategi mengatasinya? Tujuannya untuk memetakan pola kejahatan dan mengevaluasi kapasitas sistem hukum pidana dalam meresponsnya.

## B. DOKTRIN PENIPUAN DAN REZIM PEMBUKTIAN DI ERA DIGITAL

Secara doktrinal, penipuan dalam hukum pidana dibangun di atas tiga elemen utama: (1) adanya tipu muslihat atau rangkaian kebohongan, (2) adanya penyerahan barang atau uang oleh korban, dan (3) adanya hubungan kausal antara tipu muslihat dengan penyerahan tersebut (Moeljatno, 2021). Dalam konteks digital, ketiga elemen ini mengalami distorsi. Tipu muslihat tidak lagi dilakukan oleh manusia secara personal, tetapi dapat diprogram dalam bentuk algoritma, *chatbot*, atau pesan otomatis. Penyerahan tidak lagi berupa penyerahan fisik, melainkan transfer dana digital yang dapat dipicu oleh satu kali klik. Sementara kausalitas menjadi semakin kabur karena intervensi teknologi otomatis di antara pelaku dan korban.

Persoalan ini bersinggungan dengan teori pembuktian dalam hukum acara pidana. Indonesia menganut sistem pembuktian negatif berdasarkan undang-undang (*negatief wettelijk bewijsstelsel*), yang mensyaratkan sekurang-kurangnya dua alat bukti sah ditambah keyakinan hakim. Dalam penipuan digital, alat bukti elektronik yang diakui dalam Pasal 5 UU ITE menjadi kunci. Namun, bukti elektronik bersifat volatil, mudah dihapus, dan rentan terhadap manipulasi. Prinsip *chain of custody* menjadi sangat krusial, tetapi implementasinya di lapangan masih lemah karena keterbatasan kapasitas forensik digital (Santoso, 2023).

Selain itu, penipuan digital seringkali bersifat transnasional. Pelaku, server, korban, dan aliran dana berada di yurisdiksi yang berbeda. Hukum pidana tradisional dibangun di atas asas teritorialitas, yang berarti penerapannya terbatas pada wilayah negara. Keadaan ini menciptakan *jurisdictional* gap: pelaku yang berada di luar negeri sulit dijangkau, sementara ekstradisi dan bantuan hukum timbal balik seringkali berjalan lambat dan birokratis (Brenner, 2022). Kerangka teori ini akan digunakan untuk menganalisis kesenjangan antara realitas kriminal dan kapasitas sistem peradilan pidana Indonesia.

## C. MODUS OPERANDI YANG TERUS BEREVOLUSI

1. *Phishing, Smishing,* dan *Vishing*: Fondasi *Social Engineering*

*Phishing* adalah teknik pengelabuan di mana pelaku mengirimkan tautan palsu yang menyerupai situs resmi untuk mencuri kredensial korban. Evolusinya melahirkan *smishing* (melalui SMS) dan *vishing* (melalui panggilan suara). Modus terbaru yang marak di Indonesia adalah penipuan berkedok perubahan tarif transfer bank atau undangan pernikahan digital dengan ekstensi APK. Korbannya tidak lagi hanya individu yang kurang melek teknologi, melainkan juga profesional dan pebisnis. APK yang diunduh tanpa sadar akan mencuri data SMS, termasuk *one time password* (OTP) perbankan, yang memungkinkan pelaku menguras rekening

korban dalam hitungan menit. Secara teknis, ini adalah kombinasi antara phishing dan trojan yang beroperasi secara otomatis.

2. *Social Engineering* Terstruktur: Manipulasi Psikologis Sistematis

Berbeda dengan *phishing* yang bersifat massal, *social engineering* terstruktur menargetkan korban tertentu (*spear phishing*). Pelaku melakukan riset mendalam tentang target, memetakan jejaring sosialnya, dan membangun skenario yang sangat personal sehingga korban tidak menyadari sedang dimanipulasi. Modus yang paling meresahkan adalah penipuan berkedok kurir palsu, di mana pelaku menyamar sebagai petugas bank atau kepolisian dan menggunakan data pribadi korban yang sudah dicuri sebelumnya untuk meyakinkan. Korban diinstruksikan untuk memindahkan dana ke "rekening aman" dengan dalih sedang terjadi transaksi mencurigakan. Modus ini sangat efektif karena menggabungkan data bocor, tekanan psikologis, dan otoritas palsu (Mulyadi, 2023).

3. Penipuan Investasi dan *Binary Option* Ilegal

Penipuan berkedok investasi adalah salah satu yang paling merugikan secara agregat. Platform trading ilegal seperti kasus Binomo dan Quotex yang melibatkan selebriti sebagai influencer berhasil mengumpulkan dana dari ratusan ribu korban dengan janji keuntungan fantastis. Padahal, platform

tersebut hanya menampilkan simulasi grafik, sementara uang korban dialirkan ke rekening pribadi afiliator. Di sini, pelaku tidak hanya terdiri dari operator platform, tetapi juga *influencer* yang mempromosikan tanpa verifikasi. Konstruksi pertanggungjawaban pidana terhadap influencer dalam kasus semacam ini masih menjadi perdebatan: apakah mereka termasuk pelaku penipuan bersama, atau hanya sebagai korban yang tidak tahu-menahu? Putusan pengadilan terhadap kasus-kasus ini menunjukkan variasi, menandakan ketidakpastian hukum (Wibisono, 2023).

4. Deepfake dan Penipuan Berbasis AI: Ancaman Masa Depan

Pada tahap paling mutakhir, teknologi deepfake mulai digunakan untuk penipuan. Pelaku dapat memalsukan video dan suara seseorang, misalnya seorang CEO untuk memerintahkan stafnya mentransfer dana. Kasus ini sudah terjadi di luar negeri dan potensial terjadi di Indonesia karena teknologi deepfake semakin mudah diakses. Masalahnya, hukum Indonesia belum mengatur tentang pertanggungjawaban pidana penggunaan AI untuk penipuan. Apakah AI dianggap sebagai alat yang netral, atau sebagai perpanjangan dari niat jahat pelaku? Ketiadaan kerangka hukum yang jelas ini meninggalkan kekosongan yang berbahaya (Kusumawardhani, 2024).

## D. TIGA LAPIS HAMBATAN STRUKTURAL

1. Hambatan Yurisdiksi dan Anonimitas Pelaku

Sebagian besar sindikat penipuan digital besar beroperasi dari luar wilayah Indonesia. Mereka menggunakan VPN, server di negara ketiga, dan infrastruktur anonim untuk menyembunyikan jejak. Polri, dalam kapasitasnya, tidak dapat begitu saja menetapkan tersangka dan melakukan penangkapan di negara lain. Perjanjian ekstradisi dan *Mutual Legal Assistance* (MLA) ada, tetapi mekanismenya lamban. Sementara itu, Indonesia belum meratifikasi Konvensi Budapest tentang Kejahatan Siber, yang memungkinkan kerjasama lintas batas yang lebih cepat. Akibatnya, seringkali yang berhasil ditangkap hanyalah "kaki tangan" lokal, sementara otak sindikat tetap aman di luar jangkauan (ID-SIRTII, 2023).

2. Hambatan Pembuktian: *Chain of Custody* dan Bukti Digital

Pembuktian penipuan digital sangat bergantung pada bukti elektronik: *log server*, alamat IP, riwayat transaksi, dan komunikasi digital. Namun, bukti elektronik memiliki karakteristik yang rapuh. Ia mudah dihapus atau diubah jika tidak segera diamankan dengan prosedur forensik yang benar. Di Indonesia, laboratorium forensik digital masih terbatas dan terkonsentrasi di kota besar. Akibatnya, penyidik di daerah seringkali tidak

mampu memproses barang bukti digital dengan baik, sehingga perkara gagal di pengadilan karena cacat prosedural (Santoso, 2023). Selain itu, pelaku seringkali menggunakan akun fiktif yang sulit dilacak ke identitas asli. Ketiadaan regulasi yang mewajibkan registrasi identitas asli untuk nomor prabayar dan akun media sosial yang ketat membuat anonimitas menjadi tameng yang mudah bagi penipu.

3. Hambatan Pemulihan Aset: Kecepatan vs Birokrasi

Ketika korban menyadari telah ditipu dan melaporkan ke bank, dana biasanya sudah berpindah ke beberapa rekening lain dalam waktu kurang dari satu jam. Pelaku menggunakan jaringan rekening penampung (mule accounts) yang disewakan oleh pihak ketiga, yang kemudian langsung dicairkan atau dikonversi ke mata uang kripto. Kecepatan ini tidak dapat dilawan oleh mekanisme pembekuan rekening yang ada. Bank memerlukan surat resmi dari kepolisian, sementara penerbitan surat tersebut membutuhkan waktu. Belum ada mekanisme *real-time blocking* yang terintegrasi antara kepolisian, bank, dan penyedia dompet digital. Akibatnya, meskipun pelaku tertangkap, dana korban seringkali sudah tidak dapat dipulihkan (Prasetyo, 2024).

## E. POTRET KEGAGALAN DAN KEBERHASILAN PENEGAKAN HUKUM

Sindikat Penipuan Berbasis APK dan Perjuangan Pembuktian

Pada tahun 2023, publik dihebohkan dengan modus penipuan baru berupa file APK undangan pernikahan. Ribuan korban kehilangan akses rekening karena secara tidak sadar mengunduh malware yang mencuri OTP SMS. Dalam kasus ini, Polri berhasil menangkap beberapa pelaku di dalam negeri. Namun, sidang pengadilan mengungkap betapa sulitnya membuktikan keterkaitan antara pelaku yang ditangkap dengan keseluruhan jaringan. Para pelaku mengaku hanya sebagai "penjual data" atau "operator teknis" tanpa mengetahui skema besar. Kelemahan dalam digital forensic chain membuat dakwaan terbatas pada akses ilegal, bukan pada kerugian finansial total yang diderita korban. Kasus ini menunjukkan bahwa keberhasilan penangkapan tidak selalu berbanding lurus dengan keadilan substantif bagi korban (Mulyadi, 2023).

Binary Option Binomo dan Pertanggungjawaban Influencer

Kasus Indra Kenz dan Doni Salmanan menjadi landmark dalam penegakan hukum penipuan digital. Keduanya adalah influencer yang mempromosikan platform binary option ilegal Binomo dan Quotex. Mereka divonis bersalah atas penipuan dan pencucian uang, dengan pidana penjara yang cukup berat. Keberhasilan ini

menunjukkan bahwa aparat mampu menjangkau aktor-aktor yang selama ini merasa kebal hukum. Namun, kasus ini juga menyisakan pertanyaan: para influencer lainnya yang mempromosikan platform serupa, namun belum diproses secara hukum, menunjukkan adanya inkonsistensi penegakan. Selain itu, ribuan korban belum memperoleh ganti rugi yang memadai karena aset para terpidana tidak mencukupi untuk mengganti total kerugian. Sekali lagi, persoalan pemulihan aset menjadi titik lemah yang belum terpecahkan (Wibisono, 2023).

Penipuan *Business Email Compromise* (BEC) terhadap Perusahaan Ekspor

Kasus BEC menargetkan perusahaan yang melakukan transaksi internasional. Pelaku meretas surel perusahaan atau membuat surel yang sangat mirip, lalu mengirimkan instruksi pembayaran palsu. Sebuah perusahaan ekspor di Jawa Timur pernah kehilangan miliaran rupiah karena mengirimkan dana ke rekening pelaku di luar negeri atas instruksi surel yang diyakini berasal dari mitra bisnisnya. Dalam kasus ini, kendala yurisdiksi sangat terasa karena rekening tujuan berada di Hong Kong dan Tiongkok. Proses MLA yang panjang membuat pelacakan aset nyaris mustahil. Kasus BEC adalah contoh sempurna dari kejahatan transnasional yang membutuhkan kerjasama internasional yang kuat dan respons cepat yang belum dimiliki Indonesia.

## F. STRATEGI PENEGAKAN HUKUM YANG ADAPTIF DAN BERORIENTASI PEMULIHAN

Merespons tantangan-tantangan di atas, penegakan hukum penipuan digital harus mengalami transformasi fundamental. Pertama, dari sisi legislasi, perlu segera dilakukan revisi UU ITE atau pembentukan undang-undang khusus penipuan digital yang mengakomodasi perkembangan teknologi, termasuk memperjelas pertanggungjawaban penggunaan AI dan bot dalam penipuan. Unsur "tipu muslihat" dalam Pasal 378 KUHP juga perlu diinterpretasi secara lebih luas atau dilengkapi dengan delik baru yang tidak memerlukan interaksi manusia langsung.

Kedua, dari sisi kelembagaan, pembentukan direktori nasional nomor rekening penipuan yang terintegrasi secara real-time antara kepolisian, OJK, Bank Indonesia, dan seluruh penyedia jasa keuangan adalah kebutuhan yang mendesak. Direktori ini memungkinkan setiap laporan penipuan langsung memicu pembekuan dana otomatis di seluruh jaringan, sehingga memutus kecepatan pelaku. Ketiga, ratifikasi Konvensi Budapest berikut aksesi pada Protokol Tambahannya harus segera dilakukan agar Indonesia memiliki landasan hukum untuk kerjasama lintas batas yang lebih efektif, termasuk akses terhadap bukti digital yang disimpan oleh penyedia layanan di luar negeri.

Keempat, investasi besar pada forensik digital di seluruh kepolisian daerah tidak bisa ditunda. Setiap Polda harus memiliki laboratorium forensik digital yang memadai, dengan sumber daya manusia yang tersertifikasi secara internasional. Kelima, edukasi publik harus menjadi gerakan yang berkelanjutan. Kampanye "Cek Fakta, Jangan Klik" saja tidak cukup; masyarakat perlu diedukasi tentang cara melaporkan, cara mengamankan bukti, dan hak-hak mereka sebagai korban (Simanjuntak, 2024). Hanya dengan kombinasi antara represi yang cepat, pencegahan yang masif, dan pemulihan yang berorientasi korban, penipuan digital dapat ditekan ke tingkat yang terkendali.

## G. KESIMPULAN

Penipuan digital di Indonesia telah mencapai tingkat kompleksitas yang mengkhawatirkan, dengan modus operandi yang menggabungkan social engineering, otomatisasi, dan teknologi deepfake. Kerangka hukum pidana yang ada masih memiliki kelemahan fundamental pada aspek yurisdiksi, pembuktian, dan kecepatan pemulihan aset. Menjawab rumusan masalah, tantangan utama penegakan hukum terletak pada tiga lapis hambatan: yurisdiksi transnasional yang dimanfaatkan pelaku, lemahnya kapasitas forensik digital yang menggerogoti *chain of custody*, serta kecepatan aliran dana digital yang tidak dapat ditandingi oleh prosedur birokratis konvensional. Studi kasus mengkonfirmasi bahwa keberhasilan penangkapan

tidak selalu berarti keadilan bagi korban, karena pemulihan aset masih menjadi mata rantai terlemah.

Rekomendasi yang diajukan mencakup: pembentukan direktori nasional rekening penipuan dengan kemampuan pembekuan real-time, percepatan ratifikasi Konvensi Budapest, pengembangan laboratorium forensik digital di setiap Polda, revisi legislasi untuk mengakomodasi penipuan berbasis AI, serta pengarusutamaan pendidikan keamanan digital. Tanpa terobosan di bidang-bidang ini, penipuan digital akan terus menjadi *silent epidemic* yang menguras sumber daya ekonomi dan kepercayaan masyarakat terhadap ekosistem digital nasional.

**REFERENSI:**

Bareskrim Polri. (2023). Laporan Tahunan Penanganan Kejahatan Siber 2022. Jakarta: Dittipidsiber.

Brenner, S. W. (2022). Cybercrime: Criminal Threats from Cyberspace (2nd ed.). Praeger.

ID-SIRTII. (2023). Laporan Aktivitas Kejahatan Siber terhadap Pengguna Indonesia 2022. Indonesia Security Incident Response Team on Internet Infrastructure.

Kusumawardhani, A. (2024). Kecerdasan Buatan dan Kekosongan Hukum Pidana di Indonesia. Jurnal Hukum Siber, 6(1), 15–32.

Moeljatno. (2021). Asas-Asas Hukum Pidana (Edisi Revisi). Rineka Cipta.

Mulyadi, L. (2023). Social Engineering dan Evolusi Penipuan Digital: Perspektif Hukum Pidana. Jurnal Legislasi Hukum, 20(3), 412–428.

Nugroho, A. (2024). Anatomi Kejahatan Penipuan Berbasis Teknologi Digital. Jurnal Hukum Pidana dan Kriminologi, 15(1), 41–60.

Prasetyo, B. (2024). Pemulihan Aset Korban Penipuan Digital: Tantangan dan Solusi. Jurnal Hukum dan Masyarakat, 16(1), 88–107.

Santoso, L. (2023). Chain of Custody Bukti Digital dalam Sistem Peradilan Pidana Indonesia. Jurnal Yudisial, 16(3), 301–322. https://doi.org/10.29123/jy.v16i3.542

Simanjuntak, K. (2024). Literasi Keamanan Digital sebagai Pilar Ketahanan Siber Nasional. Jurnal Komunikasi dan Keamanan, 3(1), 40–58.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).

Wibisono, A. (2023). Pertanggungjawaban Pidana Influencer dalam Penipuan Investasi Ilegal.

Jurnal Pelindungan Data Pribadi dan Kejahatan Ekonomi, 2(2), 101–118.

Santoso, L. (2023). Kapasitas Forensik Digital dalam Sistem Peradilan Pidana Indonesia. Jurnal Yudisial, 16(3), 301–322. https://doi.org/10.29123/jy.v16i3.542

Shearing, C., & Wood, J. (2003). Nodal Governance, Democracy, and the New 'Denizens'. Journal of Law and Society, 30(3), 400–419. https://doi.org/10.1111/1467-6478.00263

Simanjuntak, K. (2024). Literasi Keamanan Digital sebagai Pilar Ketahanan Siber Nasional. Jurnal Komunikasi dan Keamanan, 3(1), 40–58.

Siregar, L. (2024). Investigasi Mata Uang Kripto dalam Kejahatan Ransomware. Jurnal Yudisial, 17(1), 88–105.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1,