Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 3, 2026
DOI: https://doi.org/10.61104/alz.v4i3.6634

Penggunaan Artificial Intelligence (AI) Sebagai Modus Operandi Cybercrime Dalam Tindak Pidana Penipuan Ditinjau Dari Undang-Undang ITE

Martinus Bosko Sinaga[1], Sumarno[2], Leonard[3], Maya Sari Novita[4]
Universitas Pembangunan Panca Budi Medan, Indonesia
Email Korespondensi : boskomartinus@gmail.com[1], sumarno@dosen.pancabudi.ac.id[2], leonardsimanjuntak150193@gmail.com[3], mynovita99@gmail.com [4]

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Maret 2026, Article published: 01 Juni 2026

ABSTRACT
The rapid development of information and communication technology has brought about various innovations, one of which is artificial intelligence (AI). However, despite its benefits, AI also has the potential to be misused as a means to commit crimes, particularly digital fraud. This study aims to analyze the criminal law aspects of the use of AI as a tool for fraud crimes from the perspective of the Electronic Information and Transactions Law (UU ITE). The method used is a normative juridical approach by reviewing relevant laws and regulations, legal literature, and case studies. The results indicate that although the ITE Law does not explicitly regulate the use of AI, criminal provisions in articles related to electronic fraud can be applied to perpetrators who use AI to commit fraud. Furthermore, there is an urgency for policymakers to formulate more comprehensive regulations to anticipate AI-based digital crimes. This study recommends the need for national legal updates that are adaptive to technological advances, as well as increasing the capacity of law enforcement officials to detect and handle cybercrimes involving AI.
Keywords: *Criminal Law Aspects, Artificial Intelligence (AI), Fraud*

ABSTRAK
Perkembangan teknologi informasi dan komunikasi yang pesat telah menghadirkan berbagai inovasi, salah satunya adalah kecerdasan buatan atau Artificial Intelligence (AI). Namun, di balik manfaatnya, AI juga berpotensi disalahgunakan sebagai sarana untuk melakukan tindak pidana, khususnya kejahatan penipuan berbasis digital. Penelitian ini bertujuan untuk menganalisis aspek hukum pidana terhadap penggunaan AI sebagai alat kejahatan penipuan dalam perspektif Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Metode yang digunakan adalah pendekatan yuridis normatif dengan mengkaji peraturan perundang-undangan, literatur hukum, dan studi kasus yang relevan. Hasil penelitian menunjukkan bahwa meskipun UU ITE belum secara eksplisit mengatur penggunaan AI, ketentuan pidana dalam pasal-pasal terkait penipuan elektronik dapat diberlakukan terhadap pelaku yang memanfaatkan AI untuk menipu. Selain itu, terdapat urgensi bagi pembuat kebijakan untuk merumuskan regulasi yang lebih komprehensif dalam mengantisipasi kejahatan digital berbasis AI. Penelitian ini merekomendasikan perlunya pembaruan hukum nasional yang adaptif terhadap kemajuan teknologi, serta peningkatan kapasitas aparat penegak hukum dalam mendeteksi dan menangani kejahatan siber yang melibatkan AI.
Kata Kunci: *Aspek Hukum Pidana, Artificial Intelligence (AI), Penipuan*

PENDAHULUAN

Bentuk Dan Modus Operandi Penggunaan Artificial Intelligence (AI) Dalam Tindak Pidana Penipuan Di Indonesia

Perkembangan teknologi digital di era Revolusi Industri 4.0 telah menghadirkan kemajuan pesat dalam bidang kecerdasan buatan atau Artificial Intelligence (AI). Teknologi ini memungkinkan mesin atau sistem komputer untuk melakukan tugas-tugas yang sebelumnya membutuhkan kecerdasan manusia, seperti mengenali wajah, memahami bahasa, membuat keputusan, hingga menghasilkan konten baru yang sangat menyerupai buatan manusia. AI telah menjadi bagian integral dalam kehidupan masyarakat modern dan memberikan kontribusi signifikan dalam sektor ekonomi, pendidikan, kesehatan, komunikasi, dan keamanan. Namun, bersamaan dengan manfaatnya, AI juga membawa tantangan dan risiko baru yang kompleks, terutama dalam aspek hukum dan keamanan.

Salah satu fenomena yang patut menjadi perhatian adalah penyalahgunaan teknologi AI sebagai alat untuk melakukan tindak pidana, khususnya kejahatan penipuan. Dalam konteks ini, AI tidak hanya dimanfaatkan sebagai sarana pendukung, tetapi telah bertransformasi menjadi instrumen utama dalam menjalankan modus operandi kejahatan. Contohnya, pelaku penipuan dapat menggunakan deepfake untuk memalsukan video wajah atau suara tokoh publik demi membujuk atau menipu korban; menggunakan chatbot berbasis AI untuk meniru komunikasi manusia dalam skema phishing atau investasi palsu; hingga menerapkan teknik pemrosesan bahasa alami untuk menyusun email penipuan yang sangat persuasif dan sulit dibedakan dari pesan asli.

Fenomena ini memunculkan kekhawatiran baru dalam praktik penegakan hukum. Penipuan yang dilakukan dengan bantuan AI memiliki karakteristik khusus: bersifat canggih, sulit dideteksi, dapat dilakukan lintas batas yurisdiksi, dan sering kali tidak meninggalkan jejak digital yang jelas. Bahkan, dalam beberapa kasus, pelaku kejahatan dapat menyamarkan identitas mereka sepenuhnya di balik sistem otomatis AI, sehingga menyulitkan proses identifikasi dan pembuktian di pengadilan.Di Indonesia, perbuatan penipuan secara umum diatur dalam Pasal 378 KUHP, yang merupakan produk hukum kolonial Belanda dari tahun 1918. Sementara itu, UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang diperbarui melalui UU No. 19 Tahun 2016, menjadi dasar hukum untuk menjerat pelaku kejahatan yang menggunakan media elektronik dan sistem digital. Meskipun demikian, baik KUHP maupun UU ITE belum secara eksplisit mengatur atau mengantisipasi perkembangan teknologi AI sebagai sarana atau subjek dari tindak pidana. Akibatnya, terdapat potensi kekosongan norma (legal vacuum) dan ketidakpastian hukum dalam menangani kasus-kasus penipuan berbasis AI (Ravizki & Yudhantaka, 2022).

Pertanyaan-pertanyaan penting pun muncul, Apakah AI dapat dikualifikasikan sebagai alat dalam tindak pidana sebagaimana senjata atau sarana lain dalam hukum pidana konvensional. Bagaimana konsep mens rea (niat jahat) dapat diterapkan jika sebagian tindakan dilakukan secara otomatis oleh mesin. Siapa yang dapat dimintai pertanggungjawaban pidana ketika AI bertindak atas perintah, pelatihan, atau bahkan secara otonom. Dan apakah sistem hukum pidana Indonesia

saat ini cukup adaptif dan progresif dalam menghadapi tantangan ini. Kekosongan regulasi dan keterbatasan instrumen hukum positif menjadi urgensi yang tidak dapat diabaikan. Di sisi lain, perkembangan hukum pidana harus mampu mengikuti dinamika teknologi, agar tidak tertinggal dan tetap menjamin perlindungan hukum bagi masyarakat. Oleh karena itu, diperlukan kajian yuridis yang mendalam mengenai aspek hukum pidana terhadap penggunaan Artificial Intelligence dalam kejahatan penipuan, baik dalam kerangka KUHP maupun dalam ruang lingkup UU ITE (Qurrahman et al., 2024).

Secara teoritis, hukum pidana bertujuan untuk melindungi kepentingan hukum masyarakat dari segala bentuk perbuatan yang merugikan, termasuk penipuan. Kitab Undang-Undang Hukum Pidana (KUHP) sebagai hukum pidana positif Indonesia telah mengatur perbuatan penipuan melalui Pasal 378, yang menekankan pada unsur tipu muslihat atau rangkaian kebohongan untuk memperoleh keuntungan secara melawan hukum. Di samping itu, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang telah diperbarui melalui UU Nomor 19 Tahun 2016, menjadi landasan hukum tambahan untuk menjerat tindak pidana penipuan yang dilakukan melalui media elektronik. Namun, dalam praktiknya, perkembangan teknologi informasi khususnya Artificial Intelligence (AI) menciptakan celah hukum yang cukup signifikan. Teknologi AI memungkinkan pelaku kejahatan melakukan penipuan dengan cara yang sangat canggih, seperti melalui penggunaan deepfake, voice cloning, chatbot otomatis, dan manipulasi data digital lainnya. Alat-alat ini mampu menipu korban dengan lebih meyakinkan, bahkan dalam skala yang lebih luas dan dalam waktu yang sangat singkat.

Permasalahan muncul ketika teori hukum yang ada tidak cukup adaptif terhadap modus-modus baru ini. KUHP maupun UU ITE tidak secara eksplisit mengatur mengenai penggunaan AI dalam kejahatan penipuan, sehingga penegakan hukumnya menjadi lemah atau bahkan mengalami kebingungan yuridis. Misalnya, dalam beberapa kasus, aparat penegak hukum mengalami kesulitan dalam membuktikan unsur kesengajaan dan peran pelaku manusia ketika AI digunakan sebagai alat utama kejahatan. Padahal dalam teori hukum pidana klasik, pertanggungjawaban pidana ditujukan kepada subjek hukum manusia, bukan kepada entitas teknologi (Kurniarullah et al., 2024). Kondisi ini menunjukkan adanya ketidaksesuaian antara teori hukum pidana yang berlaku dengan praktik kejahatan di lapangan. Teori pidana menekankan pertanggungjawaban pada pelaku manusia dan unsur kehendak, sementara dalam praktik, AI bisa berjalan secara otomatis atau semi-otonom berdasarkan algoritma tanpa campur tangan langsung. Hal ini menimbulkan pertanyaan mendasar yaitu siapa yang harus bertanggung jawab ketika kejahatan dilakukan dengan alat yang bekerja sendiri. Bagaimana aparat penegak hukum mengidentifikasi dan membuktikan perbuatan pidana yang dilakukan melalui AI.

Salah satu contoh kasus dari Penggunaan Artificial Intelligence (AI) Sebagai Sarana Kejahatan Penipuan terjadi di Indonesia tepatnya Pada Januari 2025, terjadi sebuah kasus penipuan berbasis deepfake Indonesia, yang menyebabkan kerugian hingga puluhan juta rupiah (Verihubs, 2025). Modus operandi kejahatan ini berupa

video manipulatif yang menampilkan Presiden Prabowo Subianto seolah-olah sedang mengumumkan program bantuan finansial dari pemerintah yang berbunyi : "Assalamualaikum masyarakat Indonesia, sebagai Presiden Indonesia, saya ingin berbagi kepada masyarakat yang sedang membutuhkan. Ini resmi dari saya pribadi, saya akan kirim masing-masing keluarga Rp 50 juta, wajib jujur untuk apa ya," demikian suara yang terdengar dalam video tersebut. Kenyataannya, Prabowo tidak pernah membuat pernyataan seperti itu. Contoh kaus kejahatan siber yang paling sering terjadi adalah penipuan daring. Kasus penipuan online terus meningkat setiap tahun, bahkan hampir selalu memakan korban setiap minggunya,dimana tingkat penyelesaian kasus tersebut masih tergolong rendah (Laia et al., 2025).

Pelaku berinisial AMA, mencantumkan nomor telepon dalam video tersebut dan meminta para korban untuk mentransfer sejumlah uang sebagai biaya administrasi awal. Jumlah yang diminta bervariasi, mulai dari Rp 250 ribu hingga Rp 1 juta. Setelah menerima pembayaran, pelaku menghilang tanpa memberikan bantuan apa pun. Setelah dilakukan penyelidikan, AMA berhasil ditangkap di rumahnya di Lampung Tengah, Provinsi Lampung, pada 16 Januari 2025. Ia dijerat dengan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Pasal 51 Ayat 1 junto Pasal 35 UU Nomor 1 Tahun 2024. Undang-undang yang merupakan revisi dari UU No. 11 Tahun 2008 tentang ITE.

Jika terbukti bersalah, AMA terancam hukuman penjara maksimal 12 tahun dan denda hingga Rp 12 miliar. Kemudian contoh selanjutnya terdapat di Jawa Timur, yaitu Polda Jatim Ungkap Kasus Penipuan Deepfake AI Kepala Daerah, Pelaku Kantongi Keuntungan Hingga Rp. 87 Juta . Para pelaku membuat sejumlah akun palsu yang menyerupai Gubernur Jawa Timur, Khofifah Indar Parawansa. Mereka memanfaatkan teknologi deepfake untuk memanipulasi video dan menyebarkannya kepada masyarakat dengan tujuan menipu. Selain Gubernur Jatim, modus serupa juga digunakan untuk mencatut nama Gubernur Jawa Barat dan Gubernur Jawa Tengah.

Fenomena ini menunjukkan urgensi akan pembaruan atau reinterpretasi terhadap konsep-konsep hukum pidana agar mampu mengakomodasi perkembangan teknologi digital. Tanpa pembaruan tersebut, terjadi jurang antara teori dan praktik yang dapat menghambat proses keadilan dan melindungi masyarakat dari bentuk kejahatan baru yang semakin kompleks. Oleh karena itu, penelitian ini bertujuan untuk mengkaji secara kritis bagaimana hukum pidana Indonesia, khususnya KUHP dan UU ITE mengatur, memahami, dan menanggapi penggunaan Artificial Intelligence sebagai sarana dalam kejahatan penipuan, serta mencari bentuk pertanggungjawaban pidana yang relevan dengan tantangan teknologi modern.

Berdasarkan uraian latar belakang di atas, maka tertarik penulis untuk mengkaji dan mengetahui lebih dalam mengenai permasalahan tersebut dalam suatu karya ilmiah berbentuk skripsi dengan judul "Aspek Hukum Pidana Terhadap Penggunaan Artificial Intelligence (AI) Sebagai Sarana Kejahatan Penipuan Dalam Perspektif UU ITE".

METODE

Metode penelitian menguraikan tentang desain penelitian, populasi dan sampel, teknik pengumpulan data, dan teknik analisis data. Penelitian kualitatif dengan studi kasus, fenomenologi, dan lainnya, setidaknya menyajikan lokasi penelitian, kehadiran peneliti, subjek penelitian, informan, dan teknik pengumpulan data penelitian, serta uraian tentang teknis analisis data penelitian (untuk penelitian kepustakaan menyebutkan jumlah literatur dan jelaskan standar pemilihan literatur sebagai objek kajian. Sedangkan pada penelitian kuantitatif, perlu disajikan populasi, sampel, dan teknik analisis data. Penelitian ini menggunakan metode penelitian hukum normatif yang merupakan bagian dari tipology penelitian doktrinal. Pendekatan penelitian yang dipakai ialah pendekatan konseptual dan perundang-undangan. Sumber data yang diperoleh dalma penelitian ini di dapat dari data skunder yang diperoleh secara tidak langsung yang merupakan studi kepustakaan dan adata skunder tersebut dibagi menjadi beberapa bagian yaitu, bahan hukum primer dan bahan hukum skunder dan bahan hukum tresier. Bahan hukum yang telah diperoleh ini kemudian di analisis menggunakan analisis deskriktif-kualitatif untuk memperoleh kesimpulan yag dapat di pertanggung jawabkan secara ilmiah terkait analisis komperatif mengenai Aspek Hukum Pidana Terhadap Penggunaan Artificial Intelligence (AI) Sebagai Sarana Kejahatan Penipuan Dalam Perspektif Undang-undang ITE

HASIL DAN PEMBAHASAN

Artificial Intelligence (AI) atau kecerdasan buatan merupakan cabang ilmu komputer yang bertujuan menciptakan sistem atau mesin yang mampu meniru kecerdasan manusia, seperti belajar, menyelesaikan masalah, mengenali pola, dan mengambil keputusan. Dalam konteks kejahatan siber (cybercrime), AI sering dimanfaatkan untuk mengotomatisasi dan menyempurnakan berbagai metode penipuan, termasuk manipulasi data, deepfake, voice cloning, dan rekayasa sosial (social engineering). John McCarthy mendefinisikan AI sebagai ilmu dan rekayasa untuk membuat mesin cerdas, terutama program komputer yang cerdas (McCarthy, n.d.). Dengan demikian, AI dapat dipahami sebagai teknologi yang dirancang untuk meniru proses berpikir manusia, baik secara mandiri maupun melalui interaksi dengan pengguna.

Secara umum, AI dibagi menjadi tiga kategori utama berdasarkan tingkat kemampuannya, yaitu Artificial Narrow Intelligence (ANI), Artificial General Intelligence (AGI), dan Artificial Super Intelligence (ASI). ANI merupakan jenis AI yang dirancang untuk menjalankan tugas tertentu secara spesifik, seperti asisten virtual, sistem rekomendasi, dan pengenalan wajah, serta telah banyak digunakan dalam kehidupan sehari-hari. AGI adalah AI yang memiliki kemampuan berpikir dan belajar setara manusia, namun hingga kini masih dalam tahap penelitian dan pengembangan. Sementara itu, ASI merupakan konsep AI masa depan yang diperkirakan memiliki kecerdasan melebihi manusia dan masih bersifat spekulatif serta menjadi perdebatan dari sisi etika maupun hukum.

Perkembangan AI menimbulkan kekhawatiran karena teknologi ini dapat dimanfaatkan untuk melakukan tindak pidana penipuan berbasis digital. AI mampu

memperluas jangkauan dan meningkatkan efektivitas kejahatan siber, seperti phishing otomatis, deepfake, voice cloning, hingga social engineering berbasis AI. Teknologi AI memungkinkan pelaku kejahatan membuat komunikasi palsu yang sangat meyakinkan sehingga korban sulit membedakan antara informasi asli dan palsu. Kondisi ini menunjukkan bahwa kemajuan teknologi tidak hanya membawa manfaat, tetapi juga menimbulkan tantangan baru dalam penegakan hukum dan keamanan digital.

Salah satu bentuk penyalahgunaan AI dalam tindak pidana penipuan adalah penggunaan teknologi deepfake dan voice cloning (Pertiwi et al., 2026). Deepfake memungkinkan pelaku membuat video atau audio palsu yang menyerupai individu tertentu, seperti pejabat, tokoh publik, maupun anggota keluarga korban. Teknologi voice cloning bahkan mampu meniru suara seseorang hanya dengan beberapa menit rekaman asli. Dalam praktiknya, pelaku dapat menghubungi korban dan berpura-pura sebagai anggota keluarga yang sedang mengalami keadaan darurat untuk meminta transfer uang. Selain itu, AI juga digunakan dalam pembuatan chatbot penipuan, email phishing yang personal, serta social engineering berbasis analisis data media sosial korban sehingga pendekatan yang dilakukan menjadi lebih efektif dan sulit dideteksi.

Penggunaan AI dalam tindak pidana penipuan di Indonesia menunjukkan bahwa kejahatan digital terus berkembang seiring kemajuan teknologi informasi. AI generatif bahkan mampu digunakan untuk membuat dokumen palsu, seperti KTP, SIM, surat perjanjian, maupun bukti transfer bank yang tampak asli. Meskipun hukum positif di Indonesia belum secara khusus mengatur penyalahgunaan AI dalam tindak pidana, penegakan hukum tetap dapat dilakukan melalui ketentuan hukum pidana umum dan hukum siber yang berlaku. Oleh karena itu, diperlukan pembaruan regulasi, peningkatan literasi digital masyarakat, serta penguatan kemampuan aparat penegak hukum agar mampu mengantisipasi berbagai bentuk penyalahgunaan AI dalam tindak pidana penipuan di masa mendatang.

Pengaturan Hukum Pidana Indonesia dalam Menanggulangi Penggunaan Artificial Intelligence (AI) Sebagai Sarana Kejahatan Penipuan di Indonesia Penipuan Dalam Perspektif Undang-undang ITE

Perkembangan teknologi informasi dan komunikasi di era revolusi industri 4.0 telah melahirkan berbagai inovasi berbasis kecerdasan buatan atau Artificial Intelligence (AI). Teknologi ini memberikan dampak positif dalam banyak aspek kehidupan, mulai dari sektor pendidikan, kesehatan, keuangan, hingga pelayanan publik. Namun di sisi lain, kemajuan teknologi ini juga menciptakan celah baru yang dimanfaatkan oleh pelaku kejahatan siber untuk melakukan tindak pidana penipuan berbasis digital.Salah satu tantangan terbesar yang dihadapi saat ini adalah munculnya modus-modus penipuan baru yang dilakukan dengan memanfaatkan kecanggihan AI, seperti penggunaan deepfake video dan suara, chatbot penipuan (scam bot), serta phishing yang dipersonalisasi oleh algoritma cerdas. Kejahatan ini sangat sulit dikenali oleh masyarakat awam karena tampil secara realistis dan meyakinkan, sehingga banyak korban yang terperdaya dan mengalami kerugian baik secara materiil maupun immateriil.

Dalam konteks hukum di Indonesia, tindak pidana penipuan telah diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) maupun Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang telah diperbarui dengan UU No. 19 Tahun 2016. Namun, pengaturan tersebut belum secara spesifik menjangkau persoalan penipuan yang dilakukan melalui sistem AI, baik dari aspek tanggung jawab pelaku, pembuktian, maupun pemidanaan.Ketiadaan regulasi khusus yang mengatur penyalahgunaan AI dalam tindak pidana menimbulkan persoalan hukum tersendiri, baik dari sisi substansi hukum, penegakan hukum, maupun perlindungan terhadap korban. Oleh karena itu, diperlukan tinjauan mendalam mengenai sejauh mana hukum pidana Indonesia mampu menanggulangi kejahatan penipuan yang menggunakan AI sebagai sarana, khususnya dalam perspektif Undang-Undang ITE sebagai dasar hukum siber nasional (Asman, 2019).

Penipuan yang menggunakan media elektronik diatur dalam: Pasal 28 ayat (1) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah oleh UU No. 19 Tahun 2016, yang berbunyi: "Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.". Pasal 45 A ayat (1) menyebutkan sanksinya: "Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00."

Pasal ini mengandung unsur inti penipuan digital, yaitu:

a. Perbuatan menyebarkan berita bohong dan menyesatkan,
b. Dilakukan dengan sengaja dan tanpa hak,
c. Mengakibatkan kerugian konsumen,
d. Terjadi dalam konteks transaksi elektronik.

Penggunaan AI dalam modus deepfake video untuk memalsukan identitas pejabat, chatbot palsu yang menawarkan produk investasi fiktif, atau phishing berbasis AI yang menyesatkan konsumen masuk dalam cakupan pasal ini. Meskipun pelaku menggunakan alat bantu AI, tanggung jawab hukum tetap dibebankan kepada subjek hukum manusia yang mengendalikannya. Saat ini Indonesia belum memiliki undang-undang khusus yang mengatur tindak pidana AI. Oleh karena itu, perlu dirumuskan Rancangan Undang-Undang Kecerdasan Artifisial, yang mengatur:

a. Etika dan larangan penggunaan AI untuk kejahatan.
b. Standar pengawasan teknologi AI.
c. Perlindungan data pribadi dari sistem berbasis AI.
d. Sanksi pidana terhadap penyalahgunaan AI.

Kecanggihan AI dalam mendukung kehidupan manusia tak dapat disangkal, namun penyalahgunaannya untuk tindak pidana penipuan menjadi ancaman nyata. Sistem hukum pidana Indonesia melalui KUHP dan UU ITE sebenarnya telah memberikan dasar normatif dalam menanggulangi kejahatan tersebut, namun masih dibutuhkan pembaruan hukum yang lebih spesifik, penguatan penegakan hukum digital, dan regulasi komprehensif terhadap AI agar mampu menjawab tantangan

masa depan. Meskipun UU ITE belum menyebutkan AI secara eksplisit, substansi hukum dalam pasal-pasal di atas mencakup unsur-unsur perbuatan penipuan yang dilakukan melalui sistem AI, baik dari segi tindakan menyebarkan kebohongan, menyesatkan masyarakat, maupun memanipulasi informasi elektronik. Oleh karena itu, UU ITE tetap menjadi payung hukum yang relevan dan aplikatif untuk menanggulangi kejahatan penipuan berbasis teknologi AI, meskipun diperlukan pembaruan regulasi yang lebih komprehensif ke depannya (Yurizal, 2015).

Pertanggungjawaban Pidana Pelaku Dalam Kasus Penipuan Online Yang Melibatkan Bantuan Kecerdasan Buatan (Artificial Intelligence)

Pertanggungjawaban pidana (criminal responsibility) merupakan konsep penting dalam hukum pidana yang merujuk pada pemberian beban hukum kepada seseorang atas perbuatan yang dianggap sebagai tindak pidana, karena orang tersebut secara sadar dan patut bertanggung jawab atas perbuatan tersebut.Secara sederhana, pertanggungjawaban pidana berarti kemampuan seseorang untuk dimintai pertanggungjawaban secara hukum atas suatu perbuatan yang dilarang oleh undang-undang pidana.

Pertanggungjawaban pidana adalah konsekuensi hukum yang dikenakan kepada pelaku tindak pidana atas perbuatan yang telah dilakukannya. Dalam hukum pidana Indonesia, terdapat unsur-unsur yang harus terpenuhi untuk dapat dikenai pertanggungjawaban pidana, yaitu:

1) Adanya perbuatan pidana (actus reus);
2) Adanya kesalahan (mens rea) berupa kesengajaan atau kelalaian;
3) Tidak adanya alasan pembenar atau pemaaf.

Tujuan dari pertanggungjawaban pidana adalah:

1) Menjamin bahwa hanya orang yang benar-benar bersalah secara hukum dan moral yang dikenai pidana;
2) Menjaga keadilan hukum, agar tidak ada orang yang dihukum atas perbuatan yang bukan tanggung jawabnya;
3) Memberikan efek jera dan edukatif, baik bagi pelaku maupun masyarakat umum.

Pertanggungjawaban pidana merupakan prinsip dasar dalam hukum pidana yang menentukan apakah seseorang dapat dikenai sanksi pidana atas perbuatannya (Fadlian, 2020). Pertanggungjawaban pidana penegakan hukuman terhadap pembuat karena perbuatan yang melanggar larangan atau menimbulkan keadaan yang terlarang. Hal ini berkaitan erat dengan niat jahat (mens rea), perbuatan yang melawan hukum (actus reus), dan kemampuan pelaku untuk memahami dan mengendalikan tindakannya. Tanpa terpenuhinya syarat-syarat tersebut, pertanggungjawaban pidana tidak dapat dibebankan kepada pelaku.

Penipuan online berbasis Artificial Intelligence (AI) merupakan bentuk kejahatan siber modern yang memanfaatkan kecerdasan buatan untuk menipu, memanipulasi, dan mengecoh korban demi memperoleh keuntungan. Dibandingkan dengan penipuan konvensional, penggunaan AI membuat modus operandi menjadi lebih canggih, terstruktur, dan sulit dideteksi. AI memungkinkan pelaku melakukan otomatisasi penipuan dalam skala besar, seperti mengirim ribuan

pesan phishing secara cepat melalui chatbot atau program otomatis. Selain itu, teknologi machine learning dan natural language processing (NLP) memungkinkan pelaku mempelajari perilaku korban sehingga pesan penipuan dapat dipersonalisasi sesuai minat, kebiasaan, dan gaya komunikasi korban. Hal ini membuat manipulasi psikologis terhadap korban menjadi lebih efektif dan sulit dikenali sebagai tindakan penipuan.

Karakteristik lain dari penipuan online berbasis AI adalah penggunaan teknologi deepfake yang mampu menciptakan gambar, suara, atau video palsu yang tampak nyata. Teknologi ini sering digunakan untuk meniru suara atasan guna memerintahkan transfer dana atau meniru wajah tokoh publik untuk mempromosikan investasi dan produk palsu. Selain itu, AI juga digunakan untuk menciptakan identitas digital palsu, seperti akun media sosial yang tampak meyakinkan lengkap dengan foto dan aktivitas layaknya akun asli. Penipuan berbasis AI juga sulit dideteksi karena sistemnya dapat beradaptasi terhadap pola keamanan digital serta memanfaatkan server luar negeri, jaringan proxy, maupun dark web untuk menghindari pelacakan aparat penegak hukum. Oleh karena itu, penipuan online berbasis AI menjadi ancaman serius yang memerlukan perhatian khusus dari masyarakat dan aparat penegak hukum.

Dalam hukum pidana Indonesia, dasar hukum pertanggungjawaban pidana terhadap penipuan online diatur dalam KUHP dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) (Siregar, 2023). Pasal 378 KUHP mengatur tentang tindak pidana penipuan yang dilakukan dengan menggunakan nama palsu, tipu muslihat, atau rangkaian kebohongan untuk menggerakkan orang lain menyerahkan barang atau uang. Ketentuan ini relevan terhadap penipuan online karena penggunaan identitas palsu dapat dilakukan melalui akun digital, situs palsu, atau media elektronik lainnya. Selain itu, Pasal 55 KUHP mengatur bahwa tidak hanya pelaku utama yang dapat dipidana, tetapi juga pihak yang membantu atau turut serta dalam tindak pidana. Dalam UU ITE, Pasal 28 ayat (1) dan Pasal 45A ayat (1) mengatur larangan penyebaran berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik, dengan ancaman pidana penjara paling lama enam tahun dan/atau denda paling banyak satu miliar rupiah.

Bentuk pertanggungjawaban pidana dalam penipuan online berbasis AI dapat berupa pertanggungjawaban sebagai pelaku langsung, penyuruh, pembantu, maupun karena kelalaian. Pelaku langsung bertanggung jawab ketika ia merancang atau mengoperasikan sistem AI untuk melakukan penipuan dan menikmati hasil kejahatan tersebut. Pertanggungjawaban juga dapat dikenakan kepada pihak yang memerintahkan orang lain untuk menjalankan sistem AI atau menyediakan sarana dan infrastruktur pendukung penipuan. Selain itu, pertanggungjawaban pidana dapat timbul karena kelalaian dalam mengawasi penggunaan AI sehingga dimanfaatkan untuk tindak pidana. Dalam konteks ini, AI hanya dipandang sebagai alat (tool), sedangkan manusia tetap menjadi subjek hukum yang bertanggung jawab atas tindak pidana penipuan online tersebut, baik secara langsung maupun tidak langsung.

SIMPULAN

Penggunaan Artificial Intelligence (AI) sebagai sarana dalam kejahatan penipuan menimbulkan tantangan baru dalam penegakan hukum pidana di Indonesia. Dalam perspektif Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), tindakan penipuan berbasis AI dapat dikategorikan sebagai pelanggaran terhadap Pasal 28 ayat (1) dan Pasal 45A ayat (1) UU ITE, yang mengatur mengenai penyebaran informasi palsu dan menyesatkan yang merugikan konsumen dalam transaksi elektronik.cAI dapat dimanfaatkan oleh pelaku untuk merekayasa informasi, menyamar sebagai pihak lain (deepfake, voice clone), atau menciptakan komunikasi palsu yang meyakinkan korban agar menyerahkan data pribadi atau melakukan transaksi yang merugikan. Walaupun UU ITE belum secara eksplisit menyebut penggunaan AI, namun unsur-unsur pidana dalam pasal-pasal tersebut tetap dapat dijadikan dasar untuk menjerat pelaku, sepanjang terpenuhi unsur kesengajaan dan kerugian yang ditimbulkan.Namun demikian, regulasi yang ada belum sepenuhnya mampu mengakomodasi kompleksitas kejahatan berbasis AI. Oleh karena itu, diperlukan pembaruan hukum dan pendekatan interpretatif oleh aparat penegak hukum agar dapat menjawab perkembangan teknologi digital secara efektif. Di samping itu, penguatan literasi digital masyarakat dan kolaborasi antar-lembaga juga menjadi elemen penting dalam mencegah dan menanggulangi kejahatan penipuan yang menggunakan AI sebagai alatnya.

DAFTAR RUJUKAN

Asman, A. (2019). *Tindak Pidana Penipuan Berbasis Transaksi Elekteronik, Guepedia*. Sinar Grafika.

Fadlian, A. (2020). Pertanggungjawaban Pidana Dalam Suatu Kerangka Teoritis. *Jurnal Hukum Positum*, *5*(2), 10–19. https://doi.org/https://doi.org/10.35706/positum.v5i2.5556

Kurniarullah, M. R., Nabila, T., Khalidy, A., Tan, V. J., & Widiyani, H. (2024). Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi Dan Pencurian Data Pribadi. *Jurnal Ilmiah Wahana Pendidikan*, *10*(10), 534–547. https://doi.org/https://doi.org/10.5281/zenodo.11448814

Laia, Y. R. N., Rahmayanti, R., Tampubolon, S. S., Gea, A. S., & Nasution, S. H. (2025). Implementasi Hukum terhadap Tindak Pidana Scammer. *JISPENDIORA :Jurnal Ilmu Sosial, Pendidikan Dan Humaniora*, *4*(1), 603–613. https://doi.org/https://doi.org/10.56910/jispendiora.v4i1.2504

McCarthy, J. (n.d.). *Apa itu AI? / Pertanyaan Dasar*. Stanford Universiti. https://jmc-stanford-edu.translate.goog/artificial-intelligence/what-is-ai/?_x_tr_sch=http&_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc

Pertiwi, W. F., Nurwati, N., & Ma'arif, R. S. (2026). Teknologi Artificial Intelligence (AI) Dalam Penipuan Berbasis Penelepon. *Jurnal Dimensi Hukum*, *10*(2), 32–37.

Qurrahman, S. H., Ayunil, S., & Rahim, T. A. (2024). Kedudukan dan Konsep Pertanggungjawaban Artificial Intelegence Dalam Hukum Positif Indonesia. *UNES Law Review*, *6*(4), 12687–12693.

https://doi.org/https://doi.org/10.31933/unesrev.v6i4.2108

Ravizki, E. N., & Yudhantaka, L. (2022). Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual dan Tantangan Pengaturan di Indonesia. *Notaire*, *5*(3), 352–380. https://doi.org/10.20473/ntr.v5i3.39063

Siregar, M. A. (2023). *Menelusuri Perjalanan Lahirnya Konsep Sistem Hukum Pidana Dan Hukum Pidana Di Indonesia*. CV Tahta Media Group.

Verihubs. (2025). *Kasus Deepfake di Indonesia: Prabowo dan Jokowi jadi Korbannya*. Verihubs. https://verihubs.com/blog/kasus-deepfake-indonesia

Yurizal, Y. (2015). *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*. Media Nusa Kreative.

