

Kajian Kriminologi Penipuan dengan Bantuan *Artificial Intelligence* dan Penegakan Hukumnya Berdasarkan UU ITE

Salsa Fardiani

Prodi Ilmu Hukum, Fakultas Hukum, Universitas Islam Bandung, Indonesia.

fardianisalsa1@gmail.com

Abstract. The development of Artificial Intelligence (AI) has had a significant impact on modern crime patterns, particularly in based fraud. Technologies such as deepfakes, voice cloning, and automated data manipulation enable perpetrators to commit fraud with high levels of accuracy and effectiveness, making it difficult to detect and potentially causing widespread losses. The research uses a normative juridical method with a legislative approach, criminology, and case analysis. Data are sourced from literature, laws and regulations, official agency reports, and concrete cases. This study examines the causal factors of AI-based crimes using theory criminology.. The results indicate that internal factors driving perpetrators include economic motives, rational calculations that AI offers high profits with low risks, and distortions of moral responsibility due to digital anonymity. External factors include the rapid advancement of accessible technology, low public digital literacy, and limited law enforcement capacity, including digital forensics. Law enforcement is carried out through the provisions of Article 492 of the New Criminal Code and articles in the ITE Law, such as Article 28 paragraph (1), Article 35, Article 51 paragraph (1), and Article 21, to ensnare the manipulation of electronic identity and information. However, its effectiveness is still hampered by the gap between technological developments and the readiness of the authorities.

Keywords: *Artificial Intelligence, Fraud, Criminology, ITE Law, Deepfake.*

Abstrak. Perkembangan Artificial Intelligence (AI) telah membawa dampak signifikan terhadap pola kejahatan modern, khususnya dalam tindak pidana penipuan. Teknologi seperti deepfake, voice cloning, dan manipulasi data otomatis memungkinkan pelaku melakukan penipuan dengan tingkat akurasi dan efektivitas tinggi, sehingga sulit dideteksi dan berpotensi menimbulkan kerugian yang luas. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, kriminologi, dan analisis kasus. Data bersumber dari literatur, peraturan perundang-undangan, laporan lembaga resmi, serta kasus konkret. Penelitian ini menelaah faktor-faktor penyebab kejahatan dengan bantuan AI melalui teori kriminologi. Bahwa faktor internal yang mendorong pelaku meliputi motif ekonomi, kalkulasi rasional bahwa AI memberikan keuntungan tinggi dengan risiko rendah, serta distorsi tanggung jawab moral akibat anonimitas digital. Adapun faktor eksternal mencakup pesatnya kemajuan teknologi yang mudah diakses, rendahnya literasi digital masyarakat, dan keterbatasan kapasitas penegakan hukum termasuk forensik digital. Penegakan hukum dilakukan melalui ketentuan Pasal 492 KUHP Baru dan pasal-pasal dalam UU ITE seperti Pasal 28 ayat (1), Pasal 35, Pasal 51 ayat (1), serta Pasal 21 untuk menjerat manipulasi identitas dan informasi elektronik. Namun, efektivitasnya masih terhambat oleh kesenjangan antara perkembangan teknologi dan kesiapan aparat.

Kata Kunci: *Artificial Intelligence, Penipuan, Kriminologi, UU ITE, Deepfake.*

A. Pendahuluan

Perkembangan teknologi kecerdasan buatan (Artificial Intelligence/AI) telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia, termasuk pada ranah ekonomi digital dan pola interaksi sosial. Di sisi lain, kemajuan teknologi tersebut juga membuka ruang baru yang dapat dimanfaatkan oleh pelaku kejahatan untuk melakukan tindak penipuan dengan memanfaatkan AI, seperti penggunaan deepfake, phishing berbasis AI, serta manipulasi data secara otomatis yang semakin sulit dikenali. Fenomena ini tidak hanya berdampak pada kerugian finansial individu, tetapi juga berpotensi merusak kepercayaan publik terhadap sistem digital secara menyeluruh.

Data survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa jumlah pengguna internet di Indonesia telah mencapai sekitar 221 juta jiwa dan terus mengalami peningkatan setiap tahunnya (Gunawan et al., 2021). Tingginya tingkat penetrasi internet tersebut secara tidak langsung memperbesar peluang terjadinya kejahatan penipuan berbasis digital, khususnya melalui media sosial, aplikasi pesan instan, serta berbagai platform keuangan digital yang semakin masif digunakan oleh masyarakat. Selain itu, laporan tahunan Digital Defense Report 2025 (MDDR 2025) mencatat bahwa selama periode Juli 2024 hingga Juni 2025, sekitar 52% serangan siber secara global didorong oleh motif keuntungan finansial. Dalam konteks kawasan Asia Pasifik, Indonesia menempati peringkat ke-12 sebagai negara dengan aktivitas siber tertinggi, dengan kontribusi sekitar 3,6% dari total aktivitas siber di wilayah tersebut. Kondisi ini menunjukkan bahwa Indonesia termasuk dalam negara yang rentan terhadap ancaman kejahatan siber, termasuk penipuan berbasis AI.

Salah satu kasus yang mencerminkan fenomena tersebut terjadi pada 28 April 2025, ketika Polda Jawa Timur mengungkap praktik penipuan dengan memanfaatkan teknologi deepfake berbasis AI yang mencatut nama sejumlah gubernur, termasuk Gubernur Jawa Timur, Khofifah Indar Parawansa. Pelaku membuat akun media sosial yang menampilkan video rekayasa berisi promosi fiktif “Program Motor Murah Seharga Rp500.000” yang seolah-olah merupakan instruksi resmi dari gubernur. Tiga orang tersangka diketahui telah menjalankan aksinya selama kurang lebih tiga bulan dengan total keuntungan mencapai sekitar Rp87.600.000. Kasus ini menunjukkan bahwa teknologi deepfake berbasis AI dapat dimanfaatkan dalam modus kejahatan daring berskala cukup besar, sehingga menuntut respons hukum yang lebih adaptif terhadap perkembangan modus kejahatan digital.

Temuan tersebut sejalan dengan penelitian yang dilakukan oleh (Fitri et al., 2025) dari Universitas Islam Bandung, yang menyatakan bahwa teknologi deepfake memiliki potensi besar untuk disalahgunakan dalam kejahatan digital, seperti penipuan dan perusakan reputasi. Deepfake dipandang sebagai bentuk ancaman baru yang menantang sistem pembuktian hukum konvensional serta perlindungan identitas digital yang selama ini berlaku.

Dalam perspektif kriminologi di Indonesia, kejahatan dipahami sebagai hasil dari interaksi kompleks antara individu dan lingkungan sosialnya (Hisyam et al., 2025). Faktor-faktor seperti tekanan sosial, ketimpangan, serta adanya kesempatan sering kali menjadi pemicu utama terjadinya perilaku kriminal. Tekanan ekonomi dan sosial dapat mendorong individu untuk melakukan tindakan menyimpang sebagai bentuk respons terhadap kondisi yang dihadapinya. Dalam konteks ini, pelaku kejahatan kerap melakukan perhitungan rasional mengenai keuntungan dan risiko sebelum melakukan tindak kriminal, termasuk dengan memanfaatkan teknologi AI guna meminimalkan kemungkinan terdeteksi sekaligus memaksimalkan keuntungan.

Konsep aktivitas rutinitas dalam kajian kriminologi juga relevan untuk menjelaskan kejahatan siber. Akses teknologi yang semakin mudah, disertai dengan lemahnya pengawasan di ruang digital, menciptakan peluang besar bagi pelaku untuk melakukan penipuan dengan tingkat risiko yang relatif rendah. Oleh karena itu, pendekatan kriminologi yang bersifat multidisipliner menekankan pentingnya integrasi aspek sosial, teknologi, dan hukum dalam memahami serta menanggulangi kejahatan siber yang terus berkembang.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) pada dasarnya disusun untuk memberikan perlindungan hukum bagi masyarakat dari kejahatan siber (Nomor, 11 C.E.). Namun, dalam praktiknya, regulasi ini dinilai belum sepenuhnya responsif terhadap perkembangan teknologi AI. Ketiadaan pengaturan yang spesifik terkait deepfake, phishing berbasis AI, serta manipulasi data otomatis menimbulkan tantangan dalam proses penegakan hukum, terutama terkait pembuktian dan persoalan yurisdiksi lintas negara. Kondisi tersebut semakin diperparah oleh

keterbatasan infrastruktur penegakan hukum, seperti minimnya kemampuan forensik digital dan lemahnya koordinasi antar lembaga, sehingga banyak kasus penipuan berbasis AI yang tidak tertangani secara optimal.

Berdasarkan kondisi tersebut, penelitian ini dipilih untuk mengisi kekosongan kajian dengan menghadirkan analisis komprehensif yang mengintegrasikan perspektif kriminologi, hukum, dan teknologi. Penelitian ini diharapkan mampu memberikan rekomendasi terkait reformasi regulasi serta strategi penegakan hukum yang lebih adaptif terhadap perkembangan teknologi AI, sehingga dapat berkontribusi dalam mengurangi dampak sosial dan ekonomi dari kejahatan penipuan berbasis digital di Indonesia.

B. Metode

Metode penelitian dalam kajian ini disusun secara sistematis untuk memperoleh pemahaman yang akurat melalui empat aspek utama, yakni metode pendekatan, spesifikasi penelitian, jenis dan teknik pengumpulan data, serta metode analisis. Pendekatan yang digunakan meliputi pendekatan perundang-undangan dan pendekatan konseptual, dengan menelaah peraturan terkait kejahatan siber seperti UU ITE dan UU Perlindungan Data Pribadi guna mengidentifikasi konsistensi serta kekosongan regulasi dalam menghadapi kejahatan penipuan berbasis AI, serta mengkaji teori-teori kriminologi seperti strain, pilihan rasional, dan aktivitas rutinitas dalam konteks hukum pidana. Penelitian ini bersifat yuridis normatif dan interdisipliner dengan karakter deskriptif-analitis, yang mengintegrasikan hukum pidana dan kriminologi untuk menggambarkan fenomena kejahatan siber berbasis AI sekaligus menganalisis efektivitas regulasi yang berlaku. Data penelitian diperoleh melalui studi pustaka dengan menggunakan sumber data primer berupa peraturan perundang-undangan dan sumber data sekunder berupa literatur hukum, kriminologi, jurnal ilmiah, serta laporan penelitian yang relevan. Selanjutnya, data dianalisis menggunakan metode kualitatif yuridis melalui interpretasi norma hukum dan teori kriminologi guna mengidentifikasi pola kejahatan, faktor penyebab, serta kendala penegakan hukum, sekaligus merumuskan rekomendasi penanganan yang adaptif terhadap perkembangan teknologi AI sesuai prinsip hukum pidana Indonesia.

C. Hasil Penelitian dan Pembahasan

Faktor Penyebab Pelaku Kejahatan Penipuan dengan Bantuan Artificial Intelligence

Kejahatan pada dasarnya dipahami sebagai perilaku menyimpang yang bertentangan dengan norma hukum maupun norma sosial yang berlaku di masyarakat. Kejahatan tidak hanya dimaknai sebagai pelanggaran terhadap ketentuan hukum tertulis, tetapi juga sebagai fenomena sosial yang lahir dari relasi antara individu dan lingkungan sosialnya. (Hisyam & MM, 2021) menyatakan bahwa kejahatan dapat terjadi ketika terdapat ketidakharmonisan antara nilai-nilai yang diyakini individu dengan nilai-nilai yang dianut oleh masyarakat, sehingga mendorong munculnya tindakan yang menyimpang dari tatanan sosial yang berlaku.

Dalam konteks masyarakat modern, bentuk dan karakter kejahatan mengalami perubahan seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi. Kejahatan tidak lagi terbatas pada aktivitas fisik di ruang nyata, melainkan juga berlangsung di ruang digital yang bersifat anonim dan melampaui batas wilayah negara. Perubahan ini menuntut pemahaman baru terhadap kejahatan sebagai fenomena yang dinamis dan terus beradaptasi dengan perkembangan sosial. (Hassan, 2017)

menegaskan bahwa suatu perbuatan hanya dapat dikategorikan sebagai kejahatan apabila telah dirumuskan secara jelas dalam peraturan perundang-undangan, sebagaimana prinsip asas legalitas dalam hukum pidana. Pandangan tersebut menempatkan kejahatan sebagai konsep yuridis yang batasannya ditentukan oleh negara melalui hukum positif. Transformasi inilah yang menjadi dasar munculnya kejahatan siber, termasuk penipuan yang dilakukan dengan bantuan Artificial Intelligence.

Salah satu jenis kejahatan yang mengalami perkembangan paling signifikan adalah kejahatan penipuan. Dalam sistem hukum pidana Indonesia, penipuan dipahami sebagai perbuatan yang dilakukan secara sengaja untuk memperoleh keuntungan secara melawan hukum melalui rangkaian tipu daya atau kebohongan yang mengakibatkan kerugian bagi pihak lain. Pengaturan mengenai

tindak pidana penipuan telah diperbarui dalam Pasal 486 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, yang pada prinsipnya menegaskan unsur kesengajaan, adanya perbuatan menipu, serta timbulnya kerugian pada korban (Nurfatlah et al., 2024).

Seiring berkembangnya teknologi digital, modus operandi penipuan juga mengalami perubahan yang signifikan. Penipuan tidak lagi dilakukan secara konvensional, melainkan memanfaatkan teknologi informasi sebagai sarana utama. Dalam konteks ini, Artificial Intelligence berperan sebagai teknologi yang mampu meningkatkan efektivitas tindak penipuan melalui rekayasa suara, gambar, video, maupun data elektronik. AI memungkinkan sistem komputer meniru proses kognitif manusia, termasuk kemampuan mengenali pola dan mengambil keputusan secara otomatis (Rojabi, 2025). Karakteristik tersebut menjadikan AI sebagai instrumen yang sangat potensial untuk disalahgunakan dalam kejahatan penipuan.

Fenomena kejahatan penipuan dengan bantuan *Artificial Intelligence* dapat dianalisis melalui beberapa teori, yaitu :

1. Teori Strain (Theory Strain)

Teori strain merupakan teori klasik dalam kriminologi yang menjelaskan bahwa kejahatan bisa terjadi karena adanya ketegangan (strain) yang dialami oleh seseorang ketika mereka tidak mampu mencapai tujuan sosial dengan cara yang sah.

2. Teori Pilihan Rasional (Rational Choice Theory)

Teori pilihan rasional menjelaskan bahwa pelaku kriminal adalah individu yang secara sadar dan rasional mempertimbangkan manfaat serta risiko sebelum melakukan suatu tindakan kriminal.

3. Teori Aktivitas Rutin (Routine Activity Theory)

Teori aktivitas rutin menjelaskan bahwa kejahatan terjadi bukan karena karakter pelaku, tetapi karena kesempatan yang terbuka.

Berdasarkan hasil analisis penulis, teori yang paling tepat untuk menjelaskan fenomena kejahatan penipuan dengan bantuan AI adalah teori pilihan rasional, karena pemanfaatan teknologi tersebut mencerminkan adanya pertimbangan yang disadari oleh pelaku. Teori ini memandang pelaku kejahatan sebagai individu yang bertindak secara rasional dengan melakukan perhitungan atas potensi keuntungan dan risiko sebelum melakukan tindak pidana. Gary S. Becker mengemukakan bahwa seseorang cenderung melakukan kejahatan ketika keuntungan yang diharapkan dipersepsikan lebih besar dibandingkan kemungkinan sanksi atau hukuman yang dapat diterimanya.

Selain itu, penerapan teori pilihan rasional juga dapat dilihat dalam praktik penipuan melalui phishing SMS yang menggunakan perangkat fake BTS. Dalam modus ini, pelaku tidak lagi mengandalkan cara-cara penipuan konvensional, melainkan memilih teknologi yang memungkinkan penyebaran pesan palsu secara luas tanpa harus melewati jaringan operator resmi. Pemilihan sarana tersebut menunjukkan adanya pertimbangan rasional dari pelaku untuk memperluas jangkauan korban sekaligus meminimalkan peluang pelacakan identitas oleh aparat penegak hukum. Kemampuan mengirim ribuan pesan dalam waktu singkat dengan biaya yang relatif rendah memperlihatkan bahwa pelaku menilai keuntungan yang diperoleh jauh lebih besar dibandingkan risiko hukum yang dihadapi.

Dalam kasus manipulasi data rekening dan pemalsuan identitas berbasis AI, teori pilihan rasional tercermin dari strategi pelaku dalam memanfaatkan sistem e-KYC dan teknologi rekayasa biometrik wajah. Pelaku secara sadar memilih AI karena teknologi ini mampu mengeksploitasi celah dalam sistem keamanan perbankan otomatis yang dirancang untuk mencegah pemalsuan identitas. Penggunaan aplikasi AI gratis yang mudah diakses di internet menunjukkan adanya perhitungan rasional untuk menekan biaya operasional kejahatan sekaligus meningkatkan peluang keberhasilan pembukaan rekening fiktif tanpa terdeteksi (Munajat & Yusuf, 2024). Hal ini menegaskan bahwa pemanfaatan AI dalam kejahatan tersebut bukan terjadi secara kebetulan, melainkan merupakan hasil kalkulasi strategis pelaku dalam memilih sarana kejahatan yang paling efektif dan efisien.

Berdasarkan kerangka pemikiran tersebut, faktor penyebab kejahatan penipuan dengan bantuan Artificial Intelligence dapat diklasifikasikan ke dalam faktor internal dan faktor eksternal, sebagaimana pandangan Soerjono Soekanto yang menempatkan kejahatan sebagai hasil interaksi antara kondisi pelaku dan lingkungan sekitarnya. Kedua faktor ini saling berkaitan dan secara bersama-sama mendorong terjadinya kejahatan penipuan berbasis teknologi.

Faktor internal berkaitan dengan motif, rasionalitas, serta sikap moral pelaku. Motif ekonomi menjadi faktor dominan, di mana pelaku terdorong untuk memperoleh keuntungan finansial secara

cepat dan signifikan. Sejalan dengan pandangan Gary S. Becker, kejahatan penipuan merupakan hasil dari keputusan rasional individu yang menilai bahwa keuntungan material yang diperoleh lebih besar dibandingkan risiko yang dihadapi. Pemanfaatan AI memungkinkan pelaku menekan biaya operasional, memperluas jangkauan korban, serta mengurangi keterlibatan fisik yang berpotensi meningkatkan risiko tertangkap, sehingga penggunaan teknologi tersebut merupakan bagian dari strategi kejahatan yang terencana. Selain itu, rendahnya kesadaran hukum dan moral pelaku turut memperkuat kecenderungan internal untuk melakukan kejahatan, di mana anonimitas dan jarak emosional yang diciptakan oleh teknologi AI menyebabkan pelaku mengalami distorsi tanggung jawab moral dan lebih mudah menormalkan perbuatannya (Budiyanto, 2025).

Faktor eksternal mencakup perkembangan teknologi, kondisi sosial, dan sistem penegakan hukum. Pesatnya perkembangan AI yang mudah diakses dan bersifat user-friendly menciptakan lingkungan yang kondusif bagi terjadinya kejahatan penipuan, bahkan oleh individu tanpa latar belakang teknis yang mendalam. Perkembangan teknologi yang tidak diimbangi dengan kesiapan sosial dan hukum memperbesar peluang penyalahgunaan AI untuk tujuan kriminal. Di sisi lain, rendahnya literasi digital masyarakat meningkatkan kerentanan korban, terutama ketika pelaku memanfaatkan konten rekayasa yang menyerupai figur publik atau institusi resmi (Febriansyah & Sh, 2025). Keterbatasan penegakan hukum, seperti minimnya kapasitas forensik digital, sumber daya manusia, serta kompleksitas kejahatan lintas wilayah, juga memperlemah efek jera dan membentuk persepsi di kalangan pelaku bahwa risiko hukum masih dapat dikendalikan.

Kejahatan penipuan berbasis Artificial Intelligence merupakan hasil interaksi yang erat antara faktor internal yang membentuk motivasi dan rasionalitas pelaku, serta faktor eksternal yang menyediakan peluang dan kondisi pendukung terjadinya kejahatan. Pemahaman yang komprehensif terhadap kedua faktor tersebut menjadi landasan penting dalam merumuskan strategi pencegahan dan penegakan hukum yang lebih adaptif, efektif, dan berkelanjutan terhadap kejahatan penipuan berbasis AI.

Upaya Penegakan Hukum Pelaku Kejahatan Penipuan dengan Bantuan Artificial Intelligence Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik

Dalam perspektif hukum pidana, penggunaan teknologi sebagai sarana kejahatan tidak menghilangkan sifat melawan hukum dari perbuatan pelaku. (Utoyo et al., 2020) menegaskan bahwa unsur kesengajaan (*dolus*) ditentukan oleh adanya kehendak dan pengetahuan pelaku dalam melakukan tindak pidana, termasuk kesadaran dalam memilih sarana untuk mencapai tujuan tersebut. Oleh karena itu, pemanfaatan Artificial Intelligence dalam penipuan justru memperkuat unsur kesengajaan, karena pelaku secara sadar menggunakan teknologi canggih untuk membangun rangkaian kebohongan yang menyesatkan korban. Dalam konteks ini, AI berfungsi sebagai *instrumentum sceleris* yang meningkatkan efektivitas kejahatan, memperluas jangkauan korban lintas wilayah dan negara, serta menimbulkan kerugian tidak hanya secara materiil, tetapi juga immateriil berupa hilangnya rasa aman dan kepercayaan masyarakat terhadap sistem digital.

Dari sudut pandang penegakan hukum pidana, kejahatan penipuan berbasis AI menunjukkan karakter kerugian yang luas dan berdampak sistemik, sehingga pendekatan non-pidana tidak lagi memadai. Hukum pidana berfungsi sebagai instrumen negara untuk melindungi kepentingan masyarakat, menegakkan norma, dan menciptakan efek jera bagi pelaku (Winatasya & Rahayuningsih, 2025). Berdasarkan analisis penulis, penegakan hukum pidana menjadi kebutuhan mendesak guna mencegah eskalasi kejahatan serupa serta memberikan perlindungan hukum yang efektif bagi masyarakat sebagai pengguna ruang digital.

Keberhasilan penegakan hukum terhadap kejahatan ini tidak terlepas dari faktor-faktor yang dikemukakan oleh Soerjono Soekanto, yakni substansi hukum, aparat penegak hukum, sarana dan prasarana, masyarakat, serta kebudayaan. Penegakan hukum tidak akan efektif apabila hanya berfokus pada norma tertulis tanpa memperhatikan kondisi sosial dan kultural yang melingkupinya. Pandangan ini sejalan dengan teori sistem hukum Lawrence M. Friedman yang menekankan pentingnya keseimbangan antara struktur hukum, substansi hukum, dan budaya hukum agar hukum dapat berfungsi secara optimal.

Dalam menganalisis penegakan hukum terhadap kejahatan penipuan dengan bantuan Artificial Intelligence (AI), penulis mengidentifikasi beberapa ketentuan peraturan perundang-undangan yang saat ini berlaku dan relevan untuk menjerat pelaku, baik dalam rezim hukum pidana

umum maupun hukum pidana khusus di bidang teknologi informasi.

Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Baru)

Tindak pidana penipuan secara normatif diatur dalam Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang KUHP Baru. Pasal ini menegaskan bahwa setiap orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum, menggunakan nama palsu, martabat palsu, tipu muslihat, atau rangkaian kebohongan sehingga orang lain menyerahkan barang, memberikan utang, atau menghapuskan piutang, dipidana karena penipuan.

Rumusan pasal tersebut menunjukkan bahwa inti delik penipuan terletak pada cara memperoleh keuntungan secara melawan hukum melalui perbuatan menipu, bukan pada alat atau sarana yang digunakan. Oleh karena itu, menurut penulis, Pasal 492 KUHP Baru tetap relevan untuk diterapkan terhadap kejahatan penipuan yang dilakukan dengan bantuan AI. Penggunaan teknologi seperti deepfake, voice cloning, maupun manipulasi identitas digital merupakan bentuk modern dari tipu muslihat atau rekayasa kebohongan yang dimaksud dalam pasal tersebut.

Meskipun Pasal 492 KUHP Baru tidak secara eksplisit menyebutkan Artificial Intelligence, unsur-unsur delik penipuan tetap terpenuhi. AI dalam konteks ini berfungsi sebagai sarana untuk menciptakan realitas palsu yang meyakinkan korban, sehingga korban secara sukarela menyerahkan harta atau data pribadinya. Dengan demikian, penggunaan AI tidak menghalangi penerapan Pasal 492 KUHP Baru terhadap pelaku.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Selain KUHP Baru, penegakan hukum terhadap kejahatan penipuan berbasis Artificial Intelligence juga harus mengacu pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024. UU ITE sebagai hukum pidana khusus (*lex specialis*) memiliki peran penting karena kejahatan penipuan berbasis AI pada umumnya dilakukan melalui sistem elektronik, media digital, dan jaringan internet.

Adapun ketentuan UU ITE yang relevan adalah sebagai berikut:

Pasal 28 ayat (1) UU ITE

Pasal 28 ayat (1) UU ITE melarang setiap orang dengan sengaja dan tanpa hak menyebarkan informasi bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. Ketentuan ini relevan dalam kasus penipuan berbasis AI, khususnya pada praktik penyebaran deepfake, pesan phishing, atau konten digital palsu lainnya yang dirancang agar tampak berasal dari pihak yang sah.

Menurut penulis, unsur “informasi bohong dan menyesatkan” terpenuhi ketika AI digunakan untuk menciptakan narasi palsu yang mempengaruhi keputusan korban dalam transaksi elektronik, sehingga menimbulkan kerugian finansial.

Pasal 35 UU ITE

Pasal 35 UU ITE mengatur larangan terhadap perbuatan memanipulasi, menciptakan, mengubah, atau menghilangkan informasi elektronik dan/atau dokumen elektronik agar dianggap seolah-olah data tersebut otentik. Pasal ini merupakan ketentuan paling krusial dalam penegakan hukum terhadap kejahatan penipuan berbasis AI.

Penggunaan deepfake, kloning suara, dan rekayasa data digital dengan bantuan AI secara substansial merupakan bentuk manipulasi informasi elektronik agar tampak autentik di mata korban. Dengan demikian, unsur perbuatan dalam Pasal 35 UU ITE terpenuhi secara jelas tanpa harus dibuktikan adanya transaksi elektronik secara langsung, selama terbukti adanya tujuan melawan hukum.

Pasal 51 ayat (1) UU ITE

Pasal 51 ayat (1) UU ITE mengatur sanksi pidana berupa pidana penjara dan/atau denda terhadap pelanggaran Pasal 35. Ketentuan sanksi ini dipertahankan dalam perubahan terakhir UU ITE melalui Undang-Undang Nomor 1 Tahun 2024.

Menurut penulis, pengaturan sanksi ini menunjukkan bahwa pembentuk undang-undang memandang manipulasi informasi elektronik sebagai perbuatan serius yang berpotensi merusak keamanan dan kepercayaan masyarakat di ruang digital, termasuk dalam kejahatan penipuan berbasis Artificial Intelligence.

Pasal 21 UU ITE

Pasal 21 UU ITE mengatur mengenai tanggung jawab hukum penyelenggara sistem elektronik untuk menjamin sistemnya beroperasi secara andal, aman, dan bertanggung jawab. Ketentuan ini relevan apabila Artificial Intelligence digunakan sebagai bagian dari sistem elektronik yang disediakan atau dikelola oleh pihak tertentu.

Berdasarkan analisis penulis, penerapan Undang-Undang Informasi dan Transaksi Elektronik Terbaru (UU Nomor 1 Tahun 2024) yang dikombinasikan dengan Kitab Undang-Undang Hukum Pidana Baru (UU Nomor 1 Tahun 2023) menunjukkan bahwa sistem hukum pidana Indonesia pada dasarnya telah memiliki dasar hukum yang memadai untuk menjerat kejahatan penipuan dengan bantuan Artificial Intelligence. Ketentuan dalam KUHP Baru digunakan untuk menjerat substansi tindak pidana penipuan dan pemalsuan, sedangkan ketentuan dalam UU ITE berfungsi untuk menjangkau sarana elektronik serta modus operandi digital yang digunakan oleh pelaku.

Meskipun hingga saat ini belum terdapat pengaturan khusus yang menempatkan Artificial Intelligence sebagai subjek hukum pidana, pendekatan kumulatif antara KUHP Baru dan UU ITE memungkinkan penegakan hukum dilakukan secara relatif komprehensif. Namun demikian, efektivitas penerapan ketentuan tersebut sangat bergantung pada kapasitas aparat penegak hukum dalam memahami perkembangan teknologi AI serta kemampuan melakukan pembuktian digital secara tepat dan akurat. Oleh karena itu, penulis berpandangan bahwa pembaruan UU ITE melalui Undang-Undang Nomor 1 Tahun 2024 merupakan langkah awal yang penting dalam merespons kejahatan berbasis teknologi. Meskipun demikian, masih diperlukan pengaturan lebih lanjut yang secara eksplisit mengatur penyalahgunaan Artificial Intelligence dalam hukum pidana Indonesia guna memberikan kepastian hukum dan meningkatkan efektivitas penegakan hukum di masa mendatang.

D. Kesimpulan

Berdasarkan hasil analisis dan pembahasan penelitian, dapat disimpulkan bahwa faktor penyebab terjadinya kejahatan penipuan dengan bantuan Artificial Intelligence berasal dari faktor internal dan faktor eksternal pelaku. Faktor internal meliputi motif ekonomi, keinginan memperoleh keuntungan secara cepat, serta pertimbangan rasional bahwa penggunaan AI memberikan efektivitas tinggi dengan risiko relatif rendah dalam mengelabui korban. Kondisi ini sejalan dengan Teori Pilihan Rasional yang memandang pelaku kejahatan sebagai individu rasional yang memilih sarana paling menguntungkan dengan hambatan seminimal mungkin. Sementara itu, faktor eksternal mencakup pesatnya perkembangan teknologi, rendahnya literasi digital masyarakat, serta keterbatasan kapasitas penegakan hukum, khususnya dalam aspek pengawasan dan forensik digital. Kombinasi faktor-faktor tersebut menciptakan ruang yang dimanfaatkan pelaku untuk melakukan penipuan secara sistematis, masif, dan lintas batas wilayah.

Penegakan hukum terhadap kejahatan penipuan berbasis Artificial Intelligence dapat dilakukan secara kumulatif melalui penerapan Pasal 492 KUHP Baru untuk menjerat unsur penipuan, serta ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU Nomor 1 Tahun 2024) untuk menindak perbuatan yang dilakukan melalui sarana elektronik. Ketentuan seperti Pasal 28 ayat (1), Pasal 35, Pasal 51 ayat (1), dan Pasal 21 UU ITE relevan dalam menanggulangi manipulasi informasi elektronik, penciptaan konten palsu yang seolah autentik, serta penyebaran informasi bohong di ruang digital. Meskipun secara normatif Indonesia telah memiliki instrumen hukum yang memadai untuk menjerat kejahatan penipuan berbasis AI, efektivitas penegakan hukum masih menghadapi kendala akibat kesenjangan antara pesatnya perkembangan teknologi dan kemampuan aparat penegak hukum dalam memahami serta membuktikan kejahatan digital.

Daftar Pustaka

- Budiyanto, S. H. (2025). Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia. Sada Kurnia Pustaka.
- Febriansyah, F. I., & Sh, M. (2025). Cybercrime: Kejahatan di Balik Layar Digital. Najaha.
- Fitri, D., Akbar, S., Mufidah, N., Manurung, R. A., Akila, D., Ramadhani, S. I., Tanjung, N. H., Putri, A., Hidayah, A. N., & Zikri, M. (2025). Deepfake Dan Krisis Kepercayaan: Analisis Hukum Terhadap Penyebaran Konten Palsu Di Media Sosial. *Jurnal Intelek Insan Cendikia*, 2(6), 11556–11568.
- Gunawan, R., Aulia, S., Supeno, H., Wijanarko, A., Uwiringiyimana, J. P., & Mahayana, D. (2021). Adiksi media sosial dan gadget bagi pengguna internet di indonesia. *Techno-Socio Ekonomika*, 14(1), 1–14.
- Hassan, M. (2017). Prinsip-prinsip keadilan hukum dalam asas legalitas hukum pidana islam. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*.
- Hisyam, C. J., & MM, M. S. (2021). Perilaku Menyimpang: Tinjauan Sosiologis. Bumi Aksara.
- Hisyam, C. J., Salsabila, A., Rahman, A. Z., Ashilah, M., Amelia, N. D., Zakaria, A., & Tampubolon,
- L. H. (2025). Analisis Motif dan Modus Kriminalitas Narapidana pada Kasus Pembegalan Melalui Studi Kasus Lapas Cipinang. *Jurnal Ilmiah Research Student*, 2(1), 51–64.
- Munajat, A. A., & Yusuf, H. (2024). Peran teknologi informasi dalam pencegahan dan pengungkapan tindak pidana ekonomi khusus: Studi tentang kejahatan keuangan berbasis digital. *Jurnal Intelek Insan Cendikia*, 1(9), 4853–4865.
- Nomor, U.-U. (11 C.E.). tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Nurfatlah, T., Abadi, S. H. K., & Efendi, S. (2024). Konsep Residive Dalam Kitab Undang-Undang Hukum Pidana Nasional Ditinjau Dalam Perspektif Tujuan Pemidanaan. *Unizar Law Review*, 7(1), 90–101.
- Rojabi, M. A. (2025). Pengantar Artificial Intelligence (AI). Afdan Rojabi Publisher.
- Utoyo, M., Afriani, K., Rusmini, R., & Husnaini, H. (2020). Sengaja Dan Tidak Sengaja Dalam Hukum Pidana Indonesia. *Lex Librum*, 7(1), 75–85.
- Winatasya, M., & Rahayuningsih, C. D. (2025). Hukum Pidana: Kajian Literature Review. *Journal of Literature Review*, 1(1), 154–160.