RECHT: JOURNAL OF LEGAL STUDIES
Volume 01 No.02, Oktober 2026
e-ISSN No. 3163-3250
Lembaga Penelitian dan Kajian Hukum, Fakultas Hukum Universitas Trisakti
This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

Tindak Pidana Penipuan Berbasis *Artificial intelligence* (AI) ditinjau dari Asas Kepastian Hukum (*Lex Certa*)

Putri Azzahra[1]

[1]*Fakultas Hukum / Universitas Islam Indonesia*
25912102@students.uii.ac.id

Abstrak

Perkembangan teknologi kecerdasan buatan *Artificial Intelligence* yang berkembang secara masih telah berimplikasi terhadap dinamika kejahatan keamanan siber, khususnya tindak pidana penipuan yang sekarang ini semakin canggih dan memiliki tingkat kesulitan yang cukup tinggi dideteksi. Pemanfaatan teknologi *deepfake* sebagai instrument penipuan telah terbukti memberikan kerugian nyata bagi masyarakat, sebagaimana tercermin dalam beberapa kasus yang terjadi di Indonesia. Penelitian ini bertukuan untuk menganalisis konstruksi hukum tindak pidana penipuan berbasis AI dalam sistem hukum pidana Indonesia serta mengkaji sejauh mana asas kepastian hukum (*lex certa*) bisa terpenuhi dalam regulasi yang berlaku. Metode yang digunakan adalah penelitian hukum normative dengan pendekatan perundang-undangan dan pendekatan konseptual melalui studi kepustakaan. Hasil penelitian menunjukan bahwa regulasi yang sudah ada dan berlaku saat ini, yakni Undang-Undang Informasi dan Transaksi Elektronik serta Pasal 492 KUHP Nasional, belum bisa menjangkau karakteristik dari kejahatan-kejahatan penipuan berbasis AI secara komprehensif. Ketidakjelasan rumusan dalam norma, kekosongan hukum, serta permasalahan pertanggungjawaban pidana menjadi hambatan utama dalam pemenuhan asas *lex certa* yang menghendaki rumusan delik bersifat jelas, tegas dan tidak multitafsis. Penelitian ini merekomendasikan perlunya suatu pemabharuan regulasi yang secara eksplisit mengakomodasi karakteristik kejahatan berbasis AI guna mewujudkan kepastian hukum yang sejati dalam sistem hukum pidana Indonesia.

Kata Kunci: *Artificial Intelligence; Deepfake;* Tindak Pidana Penipuan; Asas *Lex Certa.*

Abstract

The massive development of Artificial Intelligence (AI) technology has brought serious implications for the dynamics of cybercrime, particularly fraud offenses that are increasingly sophisticated and difficult to detect. The use of deepfake technology as an instrument of fraud has been proven to cause real harm to society, as reflected in several cases that have occurred in Indonesia. This study aims to analyze the legal construction of AI-based fraud in the Indonesian criminal law system and to examine the extent to which the principle of legal certainty (lex certa) is fulfilled in existing regulations. The method used is normative legal research with a statutory approach and a conceptual approach through literature study. The results indicate that the currently applicable regulations, namely the Electronic Information and Transactions Law and Article 492 of the National Criminal Code, have not been able to comprehensively address the unique characteristics of AI-based fraud. The ambiguity of norm formulations, legal vacuums, and problems of criminal liability constitute the main obstacles to fulfilling the lex certa principle, which requires that criminal formulations be clear, firm, and unambiguous. This study recommends the need for regulatory reform that explicitly accommodates the characteristics of AI-based crimes in order to realize genuine legal certainty within the Indonesian criminal law system.

Keywords: *Artificial Intelligenc; Deepfake; Fraud; Lex Certa Priciple.*

I. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah memasuki revolusi industry keempat yang mana memberikan sebuah revolusi digital yang membawa perubahan besar terhadap berbagai aspek kehidupan manusia. Salah satu konsekuensi mendasar dari Revolusi Industri Keempat adalah lahirnya konsep *cyber-physical systems*, yang menjembatani hubungan antara manusia dan teknologi untuk mendukung aktivitas sehari-hari secara lebih cepat, luas, dan berdampak signifikan. Konsep ini mendorong munculnya berbagai terobosan di bidang *Artificial intelligence* (AI), robotika, *Internet of Things*, kendaraan otonom, percetakan 3-D, nanoteknologi, bioteknologi, penyimpanan energi, dan komputasi kuantum yang pada akhirnya melahirkan robot-robot cerdas atau agen otonom berbasis *Artificial intelligence* (AI).[1]

Pada mulanya AI diciptakan oleh seorang ahli matematika asal Amerika bernama John McCarthy pada tahun 1955. Di samping perkembangannya yang begitu pesat dan manfaatnya yang tidak dapat dipungkiri dalam memudahkan berbagai aspek kehidupan manusia, kehadiran *Artificial Intelligence* (AI) ternyata menyimpan sisi lain yang patut mendapat perhatian serius. Kemajuan teknologi AI yang masif justru membuka celah bagi lahirnya modus-modus kejahatan baru yang semakin canggih dan sulit dideteksi. Kejahatan yang memanfaatkan teknologi digital dan jaringan siber ini dikenal dengan istilah *cybercrime*. Menurut Widodo, *cybercrime* merupakan tindak pidana yang dilakukan di dunia maya (*cyberspace*) dengan memanfaatkan teknologi informasi dan komunikasi, baik sebagai alat untuk melakukan kejahatan maupun sebagai sasaran dari kejahatan itu sendiri. Dalam konteks yang lebih luas, *cybercrime* tidak hanya mencakup serangan terhadap sistem komputer, melainkan juga meliputi penipuan elektronik, pencurian identitas digital, penyebaran konten ilegal, hingga manipulasi data yang dilakukan secara daring.[2]

Kehadiran AI telah memperluas dimensi *cybercrime* secara signifikan. Jika sebelumnya kejahatan siber mengandalkan kemampuan teknis manusia secara langsung, kini pelaku kejahatan dapat memanfaatkan AI untuk mengotomatisasi serangan, menciptakan konten palsu yang sangat meyakinkan melalui teknologi *deepfake*, mengkloning suara (*voice cloning*), hingga melancarkan penipuan massal dengan skala yang jauh lebih besar dan dalam waktu yang jauh lebih singkat.

Dengan menggunakan algoritme pembelajaran yang cukup mendalam, pelaku dapat dengan mudah meniru suara, intonasi, bahkan hingga emosi dari target hanya berdasarkan

[1] Faizin Sulistio dan Aizahra Daffa Salsasbila "Pertanggungjawaban pada Tindak Pidana yang Dilakukan Agen Otonom," *Unes Law Review* 6, No. 2 (2023): Hlm. 5481.

[2] Widodo, *Aspek Hukum Kejahatan Mayantara* (Yogyakarta: Aswindo, 2011), 7.

sample suara yang didapatkan melalui daring, biasanya digunakan atas hasil percakapan singkat, bahkan waktu yang dibutuhkan hanya tiga sampai sepuluh detik rekaman suara asli sudah cukup untuk memproses mengkloning suara yang meyakinkan. Pelaku kemudian menggunakan *voice cloning* tersebut untuk melakukan berbagai tindakan penipuan seperti permintaan transfer dana maupun interaksi palsu yang menyesatkan terhadap korban. Kasus yang sering terjadi dan melibatkan korban menerima panggilan "darurat" dimana pelaku menggunakan suara dari anggota keluarga kemudian dilakukan *cloning*, sehingga korban dapat dengan mudah tergerak untuk melakukan suatu tindakan sesuai dengan permintaan pelaku.[3]

Di Indonesia, kasus mengenai penipuan berbasis AI sudah mulai banyak dilaporkan sejak tahun 2022. Beberapa kasus yang sering dilaporkan yakni pembuatan video menggunakan teknologi *deepfake* menggunakan tokoh public demi kepentingan penipuan berkedok investasi. Contoh kasus rill, terjadi dalam kurun waktu September 2024 hingga Januari 2025, terdapat dua orang pelaku melakukan tindak pidana penipuan dengan memanfaatkan identitas milik orang lain untuk membuat rekening palsu, modus operandi yang digunakan adalah memanipulasi sistem verifikasi wajah (*biometric facial recognition*) menggunakan teknologi AI guna mengelabui protokol keamanan perbankan. Akibat aksi tersebut, pihak bank menderita kerugian besar setelah ribuan rekening fiktif berhasil diaktivasi oleh para pelaku.[4] Kasus lain yang menjadi manifestasi nyata dari ancaman ini adalah kasus penipuan yang terungkap pada Selasa, 24 Desember 2024, yang melibatkan teknik *real-time deepfake* untuk meniru identitas visual dan auditori pejabat publik. pelaku melakukan impersonasi terhadap Kapolres Jepara, AKBP Wahyu Nugroho Setyawan, dengan memanipulasi wajah dan suara melalui fitur panggilan video (*video call*). Penggunaan teknologi AI ini bertujuan untuk menciptakan otoritas palsu guna meyakinkan korban tentang kebenaran informasi yang diberikan. Modus operansi yang digunakan adalah menawarkan mobil Lelang dengan harga di bawah harga pasar, dengan mengklaim bahwa itu adalah program resmi kepolisian. Terdapat dua korban dalam kejadian ini, korban yang pertama berasal dari Jakarta dan mengalami kerugian sebesar Rp100.000.000,00 (seratus juta rupiah) serta korban yang kedua berasal dari Yogyakarta yang mengalami kerugian sebesar Rp135.000.000,00 (seratus tiga puluh lima juta rupiah).[5]

[3] Muhammad Tan Abdul Rahman Haris dan Tantimin, "Analysis of Criminal Law Liability for the Use of Artificial Intelligence in Indonesia", *Jurnal Komunikasi Hukum* (JKH), Vol. 8, No. 1 2022.

[4] "Modus Baru Penipuan Kartu Kredit dengan Aplikasi AI, 2 Pelaku Ditangkap," *Liputan6*, 7 Februari 2025, diakses 10 Agustus 2026, https://www.liputan6.com/news/read/5913070/polisi-ungkap-modus-baru-penipuan-kartu-kredit-dengan-aplikasi-ai-2-pelaku-ditangkap.

[5] "Penipuan Canggih Gunakan AI Tiru Wajah dan Suara Kapolres Jepara, Korban Rugi Ratusan Juta," *Suara Baru*, 25 Desember 2024, diakses tanggal 11 Agustus 2026, https://suarabaru.id/2024/12/25/penipuan-canggih-gunakan-ai-tiru-wajah-dan-suara-kapolres-jepara-korban-rugi-ratusan-juta.

Deepfake merupakan bukti nyata bahwa perkembangan teknologi AI saat ini mampu menciptakan dan memanipulasi konten audiovisual khususnya video secara realistis sehingga sulit dalam membedakan dari bentuk asli. Pada mulanya, teknologi ini dikembangkan untuk keperluan hiburan dan industri kreatif, namun dalam perkembangannya *deepfake* kerap disalahgunakan sebagai alat untuk melakukan suatu kejahatan, khususnya penipuan. Kondisi ini memunculkan permasalahan hukum baru yang mendesak, yakni apakah regulasi yang ada saat ini sudah mampu menjangkau karakteristik dari tindak pidana berbasis teknologi AI tersebut.

Penelitian terdahulu yang mengkaji tentang tindak pidana penipuan berbasis AI dilakukan oleh Naufal Budi Putra, Addy Candra, dan Himawan Ahmed yang berjudul "Urgensi dan Kecukukan Pengaturan Deepfake dalam Undang-Undang Informasi dan Transaksi Elektronik di Indonesia" yang membahas penggunaan Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik dalam menindak beberapa kasus yang berkaitan dengan penggunaan teknologi deepfake. Selain itu, terdapat penelitian lain dari Richo Ardi Darmawan, Ahmad Irzal dan Fristia Berdia, yang berjudul "Analisis Hukum atas Tindak Pidana Penipian Melalui Rekaman Suara Berbasis Kecerdasan Buatan (AI) dalam Perspektif Kejahatan Ekonomi" yang membahas tentang penggunaan teknologi AI berupa rekaman suara dalam melakukan tindak pidana serta menganalisis dalam perspektif ekonomi dan ketentuan hukum yang dapat digunakan untuk menindak perbuatan tersebut. Kedua penelitian tersebut pada dasarnya lebih fokus pada kecukupan pengaturan mengenai deepfake dalam Undang-Undang Informasi dan Transaksi Elektronik dan melihatnya dari perspektif kejahatan ekonomi. Sementara itu, penelitian ini berfokus pada tindak pidana penipuan berbasis AI secara lebih umum dengan meninjaunya berdasarkan asas kepastian hukum (*Lex Certa*).

Oleh karena itu, penelitian ini penting dilakukan dengan mengkaji dan menganalisis secara komprehensif bagaimana tindak pidana penipuan berbasis AI dapat dikonstuksikan dalam hukum pidana serta sejauh mana penerapannya dapat memenuhi asas kepastian hukum. Dimana hasil akhir dari penelitian ini akan memberikan pembahasan yang lebih khusus mengenai kedudukan tindak pidana penipuan dan menjawab sudah sejauh mana regulasi yang mengatur mengenai tindak pidana penipuan berbasis AI memenuhi asas kepastian hukum (*lex certa*). Argumentasi ini lah yang menjadi *novelty* dalam penelitian dan menjadi pembeda dengan penelitian-penelitian sebelumny. Oleh karena itu, peneliti melimitasi dua permasalahan utama dalam penelitian ini yakni bagaimana konstruksi hukum tindak pidana penipuan berbasis teknologi AI dalam sisten hukum pidana Indonesia? serta sejauhmana asas kepastian hukum (*lex certa*) terpenuhi dalam reguliasi yang mengatur mengenai tindak pidana penipuan berbasis teknologi AI di Indonesia?

II. Bahan Hukum dan Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif. Metode penelitian normatif merupakan proses penelitian untuk meneliti dan mengkaji tentang hukum sebagai norma, aturan, asas hukum, prinsip hukum, doktrin hukum, teori hukum serta kepustakaan lainnya untuk menjawab permalasahan hukum yang diteliti.[6] Pendekatan yang digunakan meliputi pendekatan peraturan perundang-undangan dilakukan dengan menganalisis ketentuan dalam Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 jo. Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Pendekatan konseptual digunakan untuk membangun kerangka teoritis mengenai konsep tindak pidana penipuan berbasi *Artificial Intellegence* (AI) serta konsep asas kepastian hukum (*Lex Certa*). Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer berupa peraturan perundang-undangan yang berkaitan dengan tindak pidana penipuan, penggunaan teknologi informasi, dan kecerdasan buatan, serta bahan hukum sekunder berupa buku, jurnal ilmiah, artikel hukum, dan penelitian terdahulu yang relevan. Selanjutnya, bahan hukum tersebut dianalisis secara kualitatif dengan menghubungkan ketentuan hukum yang berlaku dengan konsep dan teori hukum yang digunakan untuk memperoleh Kesimpulan mengenai peraturan tindak pidana penipuan berbasis AI dan pemenuhannya terhadap asas kepastian hukum (*Lex Certa*).

III. Hasil dan Pembahasan

Tipologi Tindak Pidana Penipuan Berbasis AI

Kemajuan teknologi yang sangat pesat ini, selain berdampak positif bagi kehidupan manusia, juga menimbulkan dampak negatif. Salah satu dampak negatif dari kemajuan teknologi saat ini, yakni munculnya kejahatan-kejahatan baru menggunakan teknologi AI. Pada perkembangannya, teknologi AI menghadirkan teknologi baru dengan sebutan *deepfake*. *Deepfake* merupakan suatu karya yang berasal dari teknologi AI yang dapat merekayasa atau memanipulasi gambar atau video menggunakan teknik *deep learning* dengan melakukan pemindaian secara menyeluruh dan mendasar terhadap bentuk manusia.[7]

Pada awalnya, deepfake hanya digunakan sebagai hiburan, namun dalam perkembangannya, deepfake disalahgunakan oleh seseorang yang tidak bertanggungjawab

[6] Muhaimin, *Metode Penelitian Hukum* (Mataram: Mataram University Press, 2020), Hlm. 48.

[7] Doni Noviantama dan Alif Alfani Rahman, "Deepfake: A Review from The Victimology Perspective," *Contemporary Issues in Criminal Law* 1, No. 2 (2024): Hlm. 111.

untuk melakukan kejahatan. Pelaku dapat dengan bebas melakukan pengeditan suatu gambar atau video wajah seseorang sesuai dengan keingannya menggunakan teknologi deepfake, yang digunakan untuk berbagai macam kejahatan salah satunya penipuan.

Menurut Gareth Shelwel, setidaknya terdapat beberapa bentuk kejahatan penipuan menggunakan teknologi AI, diantaranya peniruan identitas dengan memanipulasi wajah dan suara, penipuan yang berkaitan dengan penawaran layanan atau investasi, penipuan yang dilakukan melalui panggilan atau *videocall*, pembuatan akun media sosial palsu yang digunakan pelaku agar dapat berinteraksi dengan korban, penipuan asmara (*romance scam*), serta pengiriman email palsu (*phising*). Jika dilihat dari keenam bentuk ini, teknologi AI tidak hanya digunakan untuk suatu jenis kejahatan melainkan sudah berkembang dan dimanfaatkan dalam bentuk kepercayaan dan kelemahan terhadap korban.[8]

Jika merujuk pada bentuk-bentuk kejahatan penipuan berbasih AI yang diuraikan oleh Gareth Shelwen dan dikaitkan dengan kasus yang menjadi objek kajian dalam penelitian ini, tampak bahwa sedikitnya terdapat tiga dari enam bentuk kejahatan yang ia sebutkan terpenuhi secara bersamaan, yakni penyamaran identitas melalui rekayasa wajah dan suara, penipuan yang dilangsungkan melalui sarana *video call,* serta penipuan yang berbalut penawaran layanan dan investasi. Ketika bentuk kejahatan tersebut tidak hadir secara terpisah, melainkan digunakan dalam satu skema kejahatan secara bersamaan yang tersusun rapi, dengan menggunakan teknologi *deepfake* sebagai alat utama untuk meruntuhkan kewaspadaan dan membangun kepercayan korban sehingga penipuan dapat dilakukan hingga berhasil. Kondisi ini mempertegas bahwa kejahatan berbasis AI tidak lagi bersifat asumsi, melainkan telah hadir sebagai ancaman nyata yang secara langung menimbulkan kerugian terhadap masyarakat.

Konstruksi Hukum Pidana Penipuan Berbasis AI dalam Regulasi Indonesia

Berdasarkan penelusuran terhadap kerangka normatif yang berlaku, terdapat beberapa instrumen regulasi di Indonesia yang secara substansi relevan untuk dijadikan landasan hukum dalam penanganan tindak pidana penipuan berbasis AI, meskipun dalam praktinya masih terdapat keterbatasan dalam masing-masing regulasi tersebut.

a. Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 jo. Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik

   Undang-Undang Informasi dan Transaksi Elektronik merupakan instrumen hukum yang substansinya ditujukan untuk mengatur kejahatan siber di Indonesia,

[8] Muhammad Syafiq Wafi, Aloysius Wisnubroto, dan Yudi Prayudi, "Kejahatan Deepfake Berbasis Artificial Intelligence: Suatu Konsepsi pada Penggunaan Asas Culpabilitas Sebagai Pembaharuan Pertanggungjawaban Pidana," *Jurnal Reformasi Hukum* 29, No. 2 (2025).

namun dalam pelaksanaannya, masih terdapat beberapa celah normatif yang cukup krusial manakala dihadapkan dengan berbagai macam karakteristik tindak pidana penipuan yang memanfaatkan teknologi AI.

Pertama, dalam Undang-Undang Informasi dan Transaksi Elektronik tidak ada satupun pasal yang secara eksplisit mengatur dan menjelaskan mengenai definisi teknologi AI maupun *deepfake* sebagai suatu insturmen tindak pidana. Akibatnya, dalam penggunaan regulasi ini terhadap kasus penipuan berbasis AI sepenuhnya bergantung pada penafsiran dari aparat penegak hukum, kondisi ini berpotensi menimbulkan disparitas dalam penerapan hukum antara satu perkara dengan perkara lainnya.

Kedua, Pasal 28 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik yang substansinya mengatur mengenai penyebaran berita bohong dan menyesatkan melalui transaksi elektronik, tidak secara eksplisit mengakomodasi modus operandi penipuan berbasis AI menggunakan teknologi *deepfake video call.*

Ketiga, Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik yang substansinya mengatur mengenai pemalsuan informasi atau dokumen elektronik, secara garis besar berorientasi pada manipulasi data yang sifatnya statis. Sementara itu, kejahatan penipuan berbasis AI memiliki karakteristik yang lebih dinamis dan *real-time,* sehingga norma tersebut belum sepenuhnya dapat menjankau kondisi ini.

Keempat, Undang-Undang Informasi dan Transaksi Elektronik belum memuat aturan yang cukup mengenai mekanisme standar pembuktian khusus terhadap suatu konten yang dihasilkan melalui teknologi AI. Dalam praktiknya, membuktikan bahwa suatu video atau audio merupakan hasil dari suatu teknologi AI membutuhkan keahlian forensik digital yang spesifik[9], sementara itu regulasi mengenai standar alat bukti elektronik berbasis AI sama sekali belum terakomodasi secara noratif dalam ketentuan hukum acara pidana yang berlaku.

Kelima, Undang-Undang Informasi dan Transaksi Elektronik belum mengatur secara tegas mengenai bentuk pertanggungjawaban pidana penipuan berbasis AI. Ketiadaan norma tersebut berpotensi menimbulkan ketidakpastian hukum terkait subjek yang dapat dimintai pertanggungjawaban.

[9] Ni Putu Martina Putri, Made Sugi Hartono, dan I Dewa Gede Herman Yudiawan, "Analisis Reformulasi Pertanggungjawaban Pidana Pengguna Teknologi Deepfake Dalam Tindak Pidana Pencemaran Nama Baik Berbasis Artificial Intelligence," *Jurnal Pacta Sunt Servanda*, No. 2 (2024): Hlm. 124

Keterbatasan-keterbatasan tersebut di atas, menunjukan adanya kekosongan hukum dalam Undang-Undang Informasi dan Transaksi Elektronik, sehingga regulasi yang ada saat ini belum mampu menjangkau tindak pidana berbasis AI secara optimal.

b. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana

Pasal 492 Undang-Undang Nomor 1 Tahun 2023 merumuskan mengenai tindak pidana penipuan dengan ancaman pidana lebih berat dibandingkan dalam undang-undang sebelumnya. Sama dengan Undang Undang Informasi dan Transaksi Elektronik bahwa dalam KUHP Nasional masih terdapat beberapa keterbatasan manakala dihadapkan dengan berbagai macam karakteristik tindak pidana penipuan yang memanfaatkan teknologi AI.

Dalam Pasal 492 menyebutkan "*setiap orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau kedudukan palsu, menggunakan tipu muslihat atau rangkaian kata bohong, menggerakkan orang supaya menyerahkan suatu barang, memberi hutang, membuat pengakuan utang atau menghapus piutang dipidana karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori v"*.

Pertama, adanya keterbatasan dalam konstruksi unsur delik, dalam menentukan suatu perbuatan masuk dalam tindak pidana penipuan tentunya harus memenuhi unsur-unsur delik. Unsur "*memakai nama palsu atau kedudukan palsu"* belum mampu mengakomodasi kondisi jika penipuan dilakukan dengan menggunakan teknologi AI dengan meniru wajah dan suara miliki orang lain yang dilakukan secara *real-time*, kemudian untuk unsur lainnya seperti *"tipu muslihat atau rangkaian kata bohong",* serta *"menggerakkan orang supaya menyerahkan suatu barang"* pada dasarnya masih berorientasi pada kejahatan penipuan yang dilakukan secara konvensional yang bertumpu terhadap interakhsi secara langsung antara pelaku dan korban.

Kedua, Pasal 492 KUHP Nasional tidak menyebutkan secara eksplisit penjelasan mengenai teknologi AI maupun *deepfake* sebagai suatu sarana yang dapat digunakan dalam konstruksi tindak pidana penipuan. Ketiga, Pasal 492 KUHP Nasional belum memberikan gambaran yang cukup mengenai bagaimana hubungan sebab-akibat antara perbuatan pelaku dengan kerugian korban yang bisa dibuktikan ketika teknologi AI digunakan sebagai instrument dalam tindakan penipuan. Keempat, pada praktiknya penipuan berbasis teknologi AI ini memungkinkan dilakukan secara bersamaan terhadap korban dalam jumlah yang banyak, namun dalam pasal ini belum mengatur

secara eksplisit mengenai hal tersebut. Kelima, KUHP Nasional masih mensyarakatkan bentuk kesalahan yang dilakukan oleh subjek hukum manusia secara langsung, tentunya konsep seperti ini belum bisa memadai terhadap suatu kejahatan yang dilakukan melalui sistem yang bekerja secara otonom.

Berdasarkan keterbatasan-keterbatasan tersebut di atas, meskipun KUHP Nasional memberikan pembaharuan hukum pidana yang cukup signifikan, namun dalam Pasal 492 KUHP Nasional belum sepenuhnya mampu merespon karakteristik dari kejahatan-kejahatan berbasis AI.

Analisis Asas Kepastian Hukum (*Lex Certa*) dalam regulasi

Asas *Lex Certa* merupakan salah satu unsur legalitas dalam hukum pidana yang menekankan pentingnya kepastian hukum sebagai tujuan utama. Prinsip ini menegaskan bahwa rumusan delik dalam tindak pidana harus dirumuskan dengan jelas dan tegas sehingga tidak menimbulkan makna yang multitafsir. Konsep *Lex Certa* menempatkan kepastian hukum sebagai tujuan yang harus diwujudkan sebelum mempertimbangkan nilai-nilai hukum dalam pemidanaan terutama keadilan dan kemanfaatan.[10] Maka dari itu Kepastian hukum dari Asas *Lex Certa* mencerminkan dua fungsi utama dalam hukum pidana yaitu melindungi individu dari tindakan sewenang-wenang oleh para aparat penegakan hukum melalui regulasi yang didasarkan pada aturan jelas dan tegas serta menjamin bahwa negara berkewajiban menindak setiap perbuatan yang dikategorikan sebagai tindak pidana. Oleh sebab itu hukum pidana harus bersifat jelas dan tegas supaya dalam penerapannya tidak bertentangan dengan asas legalitas karena hukum pidana berhubungan dengan hak asasi manusia dan kebebasan individu seseorang.

Analisis terhadap regulasi yang sudah ada yakni dalam Pasal 492 KUHP Nasional dan Pasal 28 ayat (1) Undang-Undang ITE, setidaknya menunjukan terdapat beberapa permasalahan dalam aturan perkembangan teknologi AI memunculkan modus operandi baru dan belum dirumuskan secara spesifik dalam aturan tersebut sehingga para aparat penegak hukum harus menafsirkan aturan tersebut. Akibatnya terdapat ruang interprestasi yang cukup luas dalam penerapan hukum sehingga kepastian hukum yang menjadi tujuan utama dari Asas *Lex Certa* belum sepenuhnya terpenuhi, sehingga dalam penerapannya akan menimbulkan beberapa permasalahan yaitu:

a. Ketidakjelasan dalam perumusan norma, ketentuan mengenai penipuan dalam beberapa regulasi masih menggunakan terminilogi yang bersifat umum dan tidak

[10]Christovel Yamado Yacob, Problematika Penerapan Pasal 28 Ayat (2) Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik, *Jurnal Legalita* Vol. 6 No. 2, (2024), Hlm. 164.

menyebutkan secara eksplisit mengenai definisi dan penggunaan AI. Frasa seperti tipu muslihat, berita bohong, dan lain sebagainya memerlukan penafsiran yang luas agar dapat diterapkan dalam tindak pidana penipuanAI, hal ini tentu saja bertentangan dengan penerapan asas *lex certa* karena membatasi penafsiran;

b. Kekosongan norma, ketiadaan regulasi yang secara eksplisit mengatur mengenai tindak pidana penipuan yang menggunakan teknologi AI menciptakan ketidakpastian hukum yang signifikan, baik aparat penegak hukum yang perlu menentukan pasal yang tepat untuk pelaku, maupun terhadap masyarakat yang sudah sepatutnya mengetahui mengenai batasan perilaku yang dilarang;
c. Permasalahan pertanggungjawaban pidana, kompleksitas dalam penentuan subjek hukum yang dapat dimintakan pertanggungjawaban pidana ketika AI berperan sebagai "agen" yang secara mandiri melakukan penipuan.

Apabila dilihat dari perspektif teori kepastian hukum oleh Gustav Radbrunch, yang menempatkan kepastian sebagai salah satu dari tiga tujuan hukum yang saling berdampingan dengan keadilan dan kemanfaatan dapat dikatakan terlanggar. Apabila tidak ada norma yang jelas, Keputusan tentang bagaimana menangani kasus *deepfake* menjadi sangat bergantung pada siapa yang menjadi penyidik, jaksa dan hakimnya.[11] Hal ini dapat menimbulkan disparitas dalam proses penegakan hukum, baik dalam penentuan pasal yang akan diterapkan, mengidentifikasi perbuatan yang memenuhi unsur tindak pidana, maupun dalam menentukan pertanggungjawaban bagi pelaku. Akibatnya, perbuatan yang memiliki karakteristik yang serupa memiliki potensi diperlakukan secara berbeda, sehingga dapat menimbulkan ketidakpastian bagi masyarakat mengenai batasan antara perbuatan yang dilarang dan konsekuensi hukum yang akan timbul dari perbuatan tersebut. Kondisi ini menunjukan pentingnya perumusan norma mengenai tindak pidana penipuan berbasis AI yang jelas dan tegas agar dapat memberikan batasan yang pasti terhadap perbuatan yang dilarang serta mendukung penerapan asas kepastian hukum (*Lex Certa*).

Perbandingan Regulasi Internasional

Beberapa negara telah mengambil langkah yang proaktif dalam mengahadapi berbagai jenis kejahatan berbasis teknologi AI. Adapun, negara-negara maju yang saat ini sudah mempunyai aturan mengenai hal tersebut antara lain:

[11] Naufal Budi Putra Athallah, Addy Candra dan Himawan Ahmed Sanusi, "Urgensi dan Kecukupan Pengaturan Deepfake dalam Undang-Undang Informasi dan Transaksi Elektronik di Indonesia" *Judge: Jurnal Hukum*, Vol. 06 No. 09 (2026). Hlm 1672.

a. Amerika Serikat

Amerika Serikat dengan "*Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*" berlakunya peraturan ini merupakan bentuk pencegahan sebelum terjadinya tindak pidana penyalahgunaan teknologi AI dengan mengembangkan beberapa prinsip sebagai pegangan bagi semua pemangku kepenpentingan dalam kecerdasan artifisial yang memuat aturan seperti: kecerdasan AI harus aman dan terlindungi, privasi dan kebebasan sipil warga amerika serikat harus dilindungi seiiring dengan kemajuan AI, Kebijakan kecerdasan AI harus konsisten dengan dedikasi pemerintahan untuk memajukan kesetaraan dan hak-hak sipil, penting untuk mengelola risiko dari penggunaan kecerdasan AI oleh pemerintah federal sendiri dan meningkatkan kapasitas internalnya untuk mengatur, memerintah, dan mendukung penggunaan kecerdassaan AI yang bertanggung jawab untuk memberikan hasil yang lebih baik bagi warga Amerika Serikat, dan lain sebagian.[12]

b. Uni Eropa

Uni Eropa melalui *Artificial Intelligence Act* (EU AI Act) yang disahkan pada Rabu, 13 Maret 2024 oleh Parlemen Eropa,[13] menjelaskan tentang resiko sistematis terhadap penggunaan AI. Terdapat 4 (empat) kategori dalam hal resiko penggunaan AI, yakni kesatu *unacceptable risk* (bentuk risiko yang tidak dapat diterima, kedua *high risk* (bentuk risiko tinggi), ketiga *transparency risk* (bentuk risiko terbatas) dan yang keempat *minimal or no risk* (bentuk risiko minimal).[14] Meskipun jenis risiko tinggi ini diperbolehkan penggunaannya dalam EU IA Act namun terdapat beberapa larangan seperti yang dijelaskan dalam Pasal 5 ayat (1) EU AI Act bahwa terhadap beberapa penggunaan AI itu sendiri dilarang secara tegas melakukan praktik-praktik yang tidak dapat diterima karena bisa dianggap membahayakan keselamatan, mata pencaharian serta hak-hak fundamental manusia. Pasal tersebut memberikan kepastian hukum terkait pelarangan bagi pengembang maupun pengguna AI.

[12]Adzkar Ahsinin Parasurama Pamungkas, "Tata Kelola Kecerdasan Artifisial: Memetakan Inisiatif Berbagai Negara dan Organisasi Internasional" (*Jakarta: Lembaga Studi dan Advokasi Masyarakat/ELSAM*, 2023), Hlm. 14.

[13] Ugo Pagallo, Jacopo Ciani Sciolla, dan Massimo Durante, "The Environmental Challenges of AI in EU Law: Lessons Learned from the Artificial Intelligence Act (AIA) with Its Drawbacks," *Transforming Government: People, Process and Policy* 16, No. 3 (2022): 191–214.

[14] Ferio Ivan Mulyono dan Sugeng Santoso, "Permasalahan Pemutusan Hubungan Kerja melalui Artificial Intelligence (AI)," *Jurnal Private Law Fakultas Hukum Universitas Mataram* 5, no. 1 (Februari 2025): 81.

IV. Kesimpulan dan Saran

Konstruksi hukum tindak pidana penipuan berbasis Artificial Intelligence (AI) di Indonesia belum memiliki landasan normatif yang komprehensif. UU ITE dan Pasal 492 KUHP Nasional masih belum secara optimal mengakomodasi karakteristik penipuan berbasis AI, khususnya karena belum adanya pengaturan eksplisit mengenai AI dan deepfake, keterbatasan unsur delik, serta kompleksitas pembuktian dan pertanggungjawaban pidana. Kondisi tersebut menunjukkan bahwa asas kepastian hukum (*lex certa*) belum sepenuhnya terpenuhi dan berpotensi menimbulkan ketidakseragaman dalam penegakan hukum. Oleh karena itu, diperlukan pembaruan dan penguatan regulasi mengenai tindak pidana yang menggunakan teknologi AI, khususnya tindak pidana penipuan. Pembentuk undang-undang perlu mempertimbangkan pengaturan yang secara lebih jelas mengenai penggunaan Artificial Intelligence, deepfake, dan bentuk manipulasi berbasis AI lainnya yang dapat digunakan sebagai sarana melakukan tindak pidana. Pengaturan tersebut perlu memuat batasan yang jelas mengenai perbuatan yang dilarang, unsur-unsur tindak pidana, serta bentuk pertanggungjawaban pidana agar tidak menimbulkan penafsiran yang berbeda dalam proses penegakan hukum. Selain itu, perlu penguatan mekanisme pembuktian dan kemampuan aparat penegak hukum dalam menangani tindak pidana berbasis AI. Penyidik, penuntut umum, dan hakim perlu memiliki pemahaman yang memadai mengenai karakteristik teknologi AI serta metode pembuktian terhadap bukti elektronik yang berkaitan dengan tindak pidana tersebut. Dengan adanya pengaturan yang lebih jelas dan peningkatan kemampuan aparat penegak hukum, diharapkan penerapan hukum terhadap tindak pidana penipuan berbasis AI dapat dilakukan secara lebih konsisten dan tetap memperhatikan asas kepastian hukum (*lex certa*) sebagai bagian penting dalam sistem hukum pidana Indonesia.

Referensi

Buku

Muhaimin, *Metode Penelitian Hukum.* Mataram: Mataram University Press, 2020.

Pamungkas, Adzkar Ahsinin Parasurama. *Tata Kelola Kecerdasan Artifisial: Memetakan Inisiatif Berbagai Negara dan Organisasi Internasional*. Jakarta: Lembaga Studi dan Advokasi Masyarakat (ELSAM), 2023.

Widodo. *Aspek Hukum Kejahatan Mayantara*. Yogyakarta: Aswindo, 2011.

Jurnal

Ferio Ivan Mulyono dan Sugeng Santoso. "Permasalahan Pemutusan Hubungan Kerja melalui Artificial Intelligence (AI)." *Jurnal Private Law Fakultas Hukum Universitas Mataram* 5, no. 1 (2025).

Faizin Sulistio dan Aizahra Daffa Salsasbila "Pertanggungjawaban pada Tindak Pidana yang Dilakukan Agen Otonom," *Unes Law Review* 6, no. 2 (2023).

Haris, Muhammad Tan Abdul Rahmad Haris dan Tantimin. "Analisys of Criminal Law Liability for the use of Artificial Intelligence in Indonesia." *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (2022).

Naufal Budi Putra Athallah, Addy Candra, dan Himawan Ahmed Sanusi. "Urgensi dan Kecukupan Pengaturan Deepfake dalam Undang-Undang Informasi dan Transaksi Elektronik di Indonesia." *Judge: Jurnal Hukum* 6, no. 9 (2026).

Noviantama, Doni, dan Alif Alfani Rahman. "Deepfake: A Review from The Victimology Perspective." *Contemporary Issues in Criminal Law* 1, no. 2 (2024).

Pagallo, Ugo, Jacopo Ciani Sciolla, dan Massimo Durante. "The Environmental Challenges of AI in EU Law: Lessons Learned from the Artificial Intelligence Act (AIA) with Its Drawbacks." *Transforming Government: People, Process and Policy* 16, no. 3 (2022).

Putri, Ni Putu Martina, Made Sugi Hartono, dan I Dewa Gede Herman Yudiawan. "Analisis Reformulasi Pertanggungjawaban Pidana Pengguna Teknologi Deepfake Dalam Tindak Pidana Pencemaran Nama Baik Berbasis Artificial Intelligence." [*Nama Jurnal*] 5, no. 2 (2024).

Wafi, Muhammad Syafiq, Aloysius Wisnubroto, dan Yudi Prayudi. "Kejahatan Deepfake Berbasis Artificial Intelligence: Suatu Konsepsi pada Penggunaan Asas Culpabilitas Sebagai Pembaharuan Pertanggungjawaban Pidana." *Jurnal Reformasi Hukum* 29, no. 2 (2025).

Yacob, Christovel Yamado. "Problematika Penerapan Pasal 28 Ayat (2) Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik." *Jurnal Legalita* 6, no. 2 (2024).

Sumber Daring

"Modus Baru Penipuan Kartu Kredit dengan Aplikasi AI, 2 Pelaku Ditangkap." *Liputan6*, 7 Februari 2025. Diakses 18 Mei 2026. https://www.liputan6.com/news/read/5913070/polisi-ungkap-modus-baru-penipuan-kartu-kredit-dengan-aplikasi-ai-2-pelaku-ditangkap.

"Penipuan Canggih Gunakan AI Tiru Wajah dan Suara Kapolres Jepara, Korban Rugi Ratusan Juta." *Suara Baru*, 25 Desember 2024. Diakses 4 Mei 2026. https://suarabaru.id/2024/12/25/penipuan-canggih-gunakan-ai-tiru-wajah-dan-suara-kapolres-jepara-korban-rugi-ratusan-jutaz.

Peraturan Perundang-Undangan

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.