



Kualifikasi Delik dan Pertanggungjawaban Pidana terhadap Penipuan Berbasis *Deepfake* dalam KUHP Nasional

Radhin Naufal Faris¹, Daniel Sianturi², Taun³

Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Singaperbangsa Karawang

**Email: radhinnf@gmail.com*

ABSTRAK

Perkembangan kecerdasan buatan melahirkan teknologi *deepfake* yang dapat memanipulasi wajah, suara, dan video secara meyakinkan sehingga berpotensi digunakan sebagai sarana penipuan. Persoalan hukum muncul karena Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana tidak secara khusus mengatur penipuan berbasis *deepfake*, sementara penerapannya tetap harus memperhatikan asas legalitas dan larangan analogi. Penelitian ini bertujuan menganalisis penafsiran unsur delik penipuan dalam Pasal 492 serta konstruksi pertanggungjawaban pidana terhadap pihak-pihak yang terlibat. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Analisis dilakukan secara kualitatif dan preskriptif terhadap bahan hukum primer, sekunder, dan tersier. Hasil penelitian menunjukkan bahwa *deepfake* dapat menjadi sarana *tipu muslihat* apabila digunakan untuk menyesatkan korban dan menggerakkannya menyerahkan Barang atau keuntungan. Pertanggungjawaban pidana ditentukan berdasarkan peran dan kesalahan setiap pihak, sedangkan AI berkedudukan sebagai instrumen tindak pidana.

Kata Kunci: *Deepfake, Penipuan; Kualifikasi Delik, Pertanggungjawaban Pidana, KUHP Nasional*

ABSTRACT

The development of artificial intelligence has produced deepfake technology capable of convincingly manipulating faces, voices, and videos, creating opportunities for its misuse as a means of fraud. A legal issue arises because Article 492 of Law Number 1 of 2023 concerning the Criminal Code does not specifically regulate deepfake-based fraud, while its application must comply with the principle of legality and the prohibition of analogy. This research aims to examine the interpretation of fraud elements under Article 492 and the construction of criminal liability for parties involved. This normative juridical research

employs statutory, conceptual, and case approaches. Legal materials consisting of primary, secondary, and tertiary sources are analyzed qualitatively and prescriptively. The findings indicate that deepfake may constitute a means of deceit when used to mislead victims and induce them to surrender Goods or benefits. Criminal liability is determined according to the role and culpability of each party, while artificial intelligence is positioned as an instrument of the offense.

Keywords: *Deepfake, Fraud, Offense Qualification, Criminal Liability, National Criminal Code.*

INTRODUCTION

Perkembangan teknologi kecerdasan buatan selama satu dekade terakhir telah mengubah secara signifikan cara manusia memproduksi dan mengonsumsi konten digital. Salah satu hasil penting dari perkembangan tersebut ialah *deepfake*, yakni konten sintetis yang dibuat dengan memanfaatkan teknik kecerdasan buatan untuk memanipulasi wajah, suara, atau gerak tubuh seseorang, sehingga seolah-olah individu tersebut melakukan maupun menyampaikan sesuatu yang pada kenyataannya tidak pernah terjadi. Pada mulanya, teknologi *deepfake* banyak dimanfaatkan dalam bidang hiburan, industri kreatif, dan simulasi visual. Namun, kemampuannya dalam menghasilkan representasi audio-visual yang nyaris tidak dapat dibedakan dari rekaman autentik juga membuka peluang penyalahgunaan untuk merugikan pihak lain. Risiko tersebut semakin relevan dalam konteks transaksi digital yang bertumpu pada kepercayaan serta perlindungan data pengguna. Dengan demikian, kerentanan yang ditimbulkan oleh *deepfake* tidak hanya menjadi perhatian dalam bidang teknologi informasi, tetapi juga berkembang menjadi persoalan hukum, terutama dalam perspektif hukum pidana.

Penyalahgunaan teknologi *deepfake* dalam praktiknya kerap diarahkan untuk melakukan tindak pidana penipuan. Modus yang digunakan biasanya melibatkan penyamaran identitas pihak tertentu, seperti anggota keluarga korban, atasan di tempat kerja, atau figur lain yang memiliki otoritas. Penyamaran tersebut dilakukan melalui manipulasi suara maupun video untuk membangun kepercayaan semu, sehingga korban terdorong menyerahkan uang, barang, atau informasi pribadi. Dalam konteks ini, *deepfake* dapat dipahami sebagai perkembangan lebih lanjut dari pola penipuan serupa. Apabila sebelumnya identitas palsu dibentuk melalui pesan teks dan foto profil yang relatif mudah dimanipulasi, saat ini identitas tersebut dapat direkonstruksi dalam bentuk audio-visual dengan tingkat kemiripan dan kredibilitas yang jauh lebih tinggi. Kondisi tersebut pada akhirnya memperkuat kemampuan *deepfake* dalam mengecoh persepsi indrawi sekaligus memengaruhi penalaran korban.

Perkembangan modus kejahatan yang berjalan seiring dengan kemajuan teknologi pada akhirnya menghadirkan persoalan tersendiri bagi penegakan hukum pidana. Ketentuan mengenai tindak pidana penipuan dalam Pasal 492 KUHP Nasional, sebagaimana diatur dalam Undang-Undang Nomor 1 Tahun 2023, memuat sarana berupa penggunaan nama palsu, kedudukan palsu, tipu muslihat, atau rangkaian kebohongan. Rumusan tersebut secara historis merupakan warisan dari konstruksi delik penipuan klasik yang pada awalnya dibentuk untuk mengakomodasi perbuatan yang berlangsung secara langsung, tatap muka, atau menggunakan

sarana fisik. Dalam praktiknya, penegakan hukum terhadap tindak pidana penipuan menunjukkan bahwa penerapan unsur-unsur delik konvensional tersebut menghadapi tantangan seiring dengan berkembangnya modus operandi pelaku yang memanfaatkan kemajuan teknologi. Sejumlah kajian normatif mengenai penyebaran *deepfake* sebagai salah satu bentuk kejahatan siber di Indonesia memang telah dilakukan. Namun, kajian tersebut, belum secara khusus menganalisis apakah unsur-unsur delik penipuan konvensional dalam Pasal 492 KUHP Nasional.

Persoalan tersebut juga berkaitan dengan batas penafsiran yang diperbolehkan berdasarkan asas legalitas, khususnya prinsip *nullum crimen sine lege stricta* sebagaimana tercermin dalam Pasal 1 ayat (2) KUHP Nasional. Ketegangan antara rumusan norma yang bersifat relatif tetap dan karakter kejahatan yang terus mengalami perkembangan menjadi inti persoalan hukum dalam penelitian ini.

Persoalan dalam penipuan berbasis *deepfake* tidak terbatas pada kualifikasi deliknya, tetapi juga mencakup kompleksitas dalam menentukan pertanggungjawaban pidana. Dalam penipuan konvensional, pelaku pada umumnya melakukan perbuatan secara langsung. Sebaliknya, skema *deepfake* dapat melibatkan beberapa pihak dengan peran yang berbeda, mulai dari pembuat konten sintetis, pihak yang menyebarkan konten tersebut, hingga pihak yang secara aktif memanfaatkannya untuk mendorong korban menyerahkan sesuatu. Kondisi ini menimbulkan pertanyaan mengenai batas pertanggungjawaban pidana setiap pihak dalam kerangka penyertaan (*deelneming*). Kompleksitas tersebut semakin meningkat karena hukum pidana Indonesia, termasuk KUHP Nasional sebagaimana diatur dalam Undang-Undang Nomor 1 Tahun 2023, belum menempatkan kecerdasan buatan sebagai subjek hukum yang dapat dimintai pertanggungjawaban pidana secara mandiri. Dengan demikian, sistem kecerdasan buatan yang digunakan untuk menghasilkan konten *deepfake* pada dasarnya tetap dipandang sebagai sarana atau instrumen kejahatan, bukan sebagai pelaku tindak pidana.

Ketiadaan pengaturan yang secara khusus mengatur atribusi tindak pidana yang melibatkan kecerdasan buatan menjadi salah satu persoalan penting dalam upaya membangun tata kelola kecerdasan buatan yang etis, termasuk untuk mencegah penyalahgunaan teknologi tersebut dalam penyebaran informasi atau konten palsu. Persoalan mengenai pertanggungjawaban pidana ini menjadi isu lanjutan yang perlu dianalisis setelah kualifikasi penipuan berbasis *deepfake* dapat dibuktikan secara meyakinkan.

Berdasarkan uraian tersebut, penelitian ini berfokus pada dua permasalahan utama. Pertama, penelitian menganalisis penafsiran unsur-unsur tindak pidana penipuan dalam Pasal 492 KUHP Nasional terhadap modus operandi yang memanfaatkan teknologi *deepfake*. Kedua, penelitian mengkaji batas pertanggungjawaban pidana para pihak yang terlibat dalam skema penipuan tersebut. Kedua permasalahan tersebut akan dibahas secara sistematis dan berurutan pada bagian pembahasan.

METHOD

Penelitian ini menggunakan metode penelitian hukum normatif atau yuridis normatif yang menempatkan norma hukum sebagai objek utama kajian. Penelitian diarahkan untuk menganalisis konstruksi hukum pidana terhadap penipuan berbasis teknologi *deepfake*, khususnya terkait penafsiran unsur-unsur Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana serta pertanggungjawaban pidana pihak-pihak yang terlibat dalam pelaksanaannya. Karakter penelitian yang bersifat normatif dipilih karena permasalahan yang dikaji berkenaan dengan norma, asas, konsep, dan doktrin hukum yang digunakan untuk menentukan kualifikasi delik serta dasar pertanggungjawaban pidana dalam hukum pidana Indonesia.

Penelitian ini menggunakan pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan digunakan dengan menelaah Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana beserta peraturan perundang-undangan lain yang memiliki keterkaitan dengan tindak pidana penipuan, teknologi informasi, dan penggunaan teknologi kecerdasan buatan. Pendekatan konseptual digunakan untuk mengkaji konsep penipuan, kesalahan, kesengajaan, pertanggungjawaban pidana, penyertaan (*deelneming*), dan pembantuan (*medeplichtigheid*) sebagai dasar untuk menentukan kedudukan hukum pihak-pihak yang terlibat dalam penipuan berbasis *deepfake*. Pendekatan kasus digunakan dengan menelaah putusan pengadilan dan perkara yang relevan dengan penipuan, manipulasi identitas digital, atau penggunaan teknologi sebagai sarana tindak pidana untuk melihat penerapan unsur delik dan pertanggungjawaban pidana oleh aparat penegak hukum.

Bahan hukum penelitian terdiri atas bahan hukum primer, sekunder, dan tersier yang dikumpulkan melalui studi kepustakaan (*library research*). Bahan hukum primer mencakup Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, serta peraturan perundang-undangan terkait; bahan hukum sekunder meliputi buku hukum pidana, jurnal ilmiah terakreditasi, hasil penelitian, doktrin, dan pendapat sarjana yang relevan; sedangkan bahan hukum tersier berupa kamus hukum, kamus bahasa, dan ensiklopedia yang digunakan untuk memperjelas istilah tertentu. Analisis dilakukan secara kualitatif dengan sifat preskriptif melalui penalaran deduktif, yaitu menghubungkan ketentuan hukum yang bersifat umum dengan karakteristik penipuan berbasis *deepfake* untuk menilai pemenuhan unsur Pasal 492 KUHP Nasional, kemudian mengidentifikasi peran, kesalahan, dan kontribusi setiap pihak berdasarkan ketentuan mengenai pelaku, penyertaan, pembantuan, serta pertanggungjawaban pidana.

RESULT AND DISCUSSION

Hasil Penelitian

1. **Bagaimana Penafsiran Unsur-unsur Delik Penipuan dalam Pasal 492 KUHP Nasional Terhadap Modus Operandi Berbasis Teknologi *Deepfake*?**

Dalam hukum pidana, istilah delik diserap dari *strafbaar feit* dalam doktrin Belanda. Istilah lain juga digunakan dalam mengartikan delik yaitu *delic* yang berasal dari bahasa latin yakni *delictum* yang kemudian dipakai dalam bahasa Indonesia sebagai istilah delik. Moeljatno menyatakan bahwa tindak pidana adalah perbuatan yang dilarang oleh suatu aturan hukum yang disertai ancaman pidana bagi siapa yang melanggarnya. Simons merumuskan delik sebagai tindakan melanggar hukum yang dilakukan dengan sengaja maupun tidak sengaja oleh seseorang yang dapat dipertanggungjawabkan atas perbuatannya, dan oleh undang-undang telah dinyatakan sebagai perbuatan yang dapat dihukum, dengan tiga unsur pokok: adanya suatu perbuatan manusia, perbuatan itu dilarang dan diancam hukuman oleh undang-undang, serta perbuatan itu dilakukan oleh orang yang dapat dipertanggungjawabkan.

Aturan mengenai delik penipuan diatur dalam pasal 492 KUHP Nasional (Undang – Undang No. 1 Tahun 2023) yang berbunyi: “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 utang, membuat pengakuan utang, atau menghapus piutang, dipidana karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori V”. Berdasarkan isi pasal tersebut, terdapat delik yang memuat unsur subjektif dan unsur objektif. Unsur subjektif bermakna menguntungkan diri sendiri atau orang lain secara melawan hukum. Sedangkan unsur objektif tersusun dari dua alternatif, yaitu (pertama) sarana yang digunakan pelaku memakai nama palsu, kedudukan palsu, tipu muslihat, atau rangkaian kata bohong, dan (kedua) akibat yang dituju dari sarana tersebut yang menggerakkan korban untuk melakukan apa yang diinginkan pelaku dengan niat jahat.

Deepfake merupakan bagian dari konten sintetis yang menggunakan kecerdasan buatan untuk menciptakan konten yang membuat orang terlihat atau terdengar melakukan hal-hal yang sebenarnya tidak dilakukan. Secara umum, *deepfake* bekerja melalui manipulasi identitas visual seseorang yang direalisasikan melalui model generatif sehingga menghasilkan konten yang bisa saja sebenarnya tidak pernah dilakukan. Hal inilah yang membuat *deepfake* memiliki potensi dampak negatif jika disalahgunakan untuk penipuan. Maka dari itu, penipuan menggunakan *deepfake* menjadi fenomena yang perlu menjadi perhatian dalam literatur hukum di Indonesia.

Merujuk pada dua lapis unsur objektif Pasal 492 KUHP Nasional sebagaimana telah dijelaskan, konten *deepfake* dapat diuji berdasarkan dua sarana yang bersifat alternatif. Sarana pertama adalah tipu muslihat. Dalam hukum pidana, tipu muslihat pada umumnya dipahami sebagai suatu perbuatan yang menciptakan keadaan atau penampilan tertentu sehingga dapat menyesatkan indra korban. Pengertian ini berbeda dengan rangkaian kata bohong, yang lebih menekankan pada penyampaian informasi palsu secara verbal. Karakteristik *deepfake* untuk menghasilkan representasi visual dan/atau audio yang secara meyakinkan menampilkan seseorang seolah-olah melakukan atau mengatakan sesuatu yang sebenarnya tidak pernah terjadi, pada dasarnya sejalan dengan pengertian tipu muslihat tersebut. Dalam *deepfake*, pelaku tidak hanya menyampaikan kebohongan melalui kata-kata, tetapi juga merekayasa tampilan

visual atau suara yang dapat diterima oleh indra korban. Akibatnya, korban dapat mempercayai suatu keadaan yang tampak nyata, padahal keadaan tersebut sebenarnya palsu dan telah dimanipulasi oleh pelaku.

Poin utamanya terletak pada batas antara penafsiran ekstensif yang sah dan analogi yang dilarang dalam hukum pidana. Asas legalitas (pasal 1 ayat (2) KUHP Nasional) melarang penetapan adanya tindak pidana dengan didasarkan pada analogi, yakni menerapkan norma pada perbuatan yang secara substansial berbeda dari yang dimaksud undang – undang. Maka timbul pertanyaan mengenai hal tersebut, yaitu Apakah istilah “tipu muslihat” yang secara historis dipahami sebagai tindakan langsung untuk menciptakan keadaan fisik yang menyesatkan indra korban, masih dapat mencakup konten sintetis yang dibuat melalui sistem algoritmik generatif?

Pertanyaan tersebut sebenarnya telah memiliki pijakan awal dalam praktik peradilan Indonesia. Kasus penipuan berkedok cinta melalui aplikasi kencan daring Tinder dalam Putusan Pengadilan Negeri Surabaya Nomor 2414/Pid.B/2020/PN.SBY menunjukkan bahwa perkembangan teknologi digital telah dimanfaatkan pelaku kejahatan untuk melakukan penipuan melalui pembangunan persona palsu secara daring. Meskipun pelaku tidak bertemu langsung dengan korban dan tidak menggunakan dokumen fisik, pengadilan tetap menerapkan unsur delik penipuan konvensional terhadap perbuatan tersebut.

Berdasarkan temuan tersebut (Putusan Pengadilan Negeri Surabaya Nomor 2414/Pid.B/2020/PN.SBY), penulis berpendapat bahwa alasan penafsiran yang sama dapat diterapkan terhadap modus *deepfake*. Jika pengadilan telah mengakui bahwa persona palsu yang dibangun melalui teks dan foto profil di internet seperti dalam kasus penipuan berkedok cinta melalui Tinder dapat memenuhi unsur tipu muslihat, maka konten *deepfake* seharusnya juga termasuk dalam cakupan penafsiran tersebut. *Deepfake* bahkan memiliki kemampuan yang lebih besar untuk menyesatkan korban karena dapat memanipulasi suara dan gambar secara meyakinkan. Perbedaan antara persona palsu dalam kasus Tinder dan *deepfake* terutama terletak pada tingkat kecanggihan teknologi yang digunakan, bukan pada inti perbuatannya. Keduanya sama-sama menciptakan keadaan atau tampilan palsu yang dapat memengaruhi persepsi korban. Oleh karena itu, penerapan unsur tipu muslihat terhadap modus *deepfake* tidak dapat dianggap sebagai penafsiran yang terlalu jauh dari praktik peradilan yang telah ada. Penerapan tersebut justru merupakan kelanjutan logis dari pola penafsiran yang sebelumnya telah diterima pengadilan terhadap tindak penipuan yang dilakukan melalui teknologi digital.

2. Bagaimana Konstruksi Pertanggungjawaban Pidana terhadap Pihak-Pihak yang Terlibat dalam Tindak Pidana Penipuan Berbasis *Deepfake* dalam Kerangka Hukum Pidana Indonesia Pascaberlakunya KUHP Nasional?

Penggunaan teknologi *deepfake* dapat melibatkan beberapa tahapan perbuatan dan lebih dari satu pihak sebelum penipuan terhadap korban benar-benar terlaksana. Kondisi tersebut relevan dengan konstruksi penyertaan yang telah diatur oleh KUHP Nasional karena kedudukan setiap orang yang terlibat tidak selalu dapat dipersamakan sebagai pelaku utama. Pasal 20 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana mengatur beberapa bentuk

pelaku tindak pidana, yaitu orang yang melakukan tindak pidana seorang diri, melakukan tindak pidana melalui perantara alat atau orang yang tidak dapat dipertanggungjawabkan, turut serta melakukan tindak pidana, atau menggerakkan orang lain untuk melakukan tindak pidana. Keberadaan teknologi *deepfake* tidak dengan sendirinya membentuk pola pertanggungjawaban pidana yang berbeda dari prinsip atribusi yang berlaku, tetapi teknologi tersebut dapat memengaruhi cara suatu tindak pidana dilaksanakan serta hubungan fungsional antara pihak-pihak yang memberikan kontribusi terhadap terwujudnya perbuatan pidana.

Penentuan pihak yang dapat dimintai pertanggungjawaban terlebih dahulu memerlukan pembedaan antara kecerdasan buatan sebagai instrumen dan manusia sebagai subjek hukum pidana. KUHP Nasional menggunakan subjek “Setiap Orang” sebagai pihak yang dapat dikenai pertanggungjawaban pidana, sedangkan Pasal 36 ayat (1) mensyaratkan adanya kesengajaan atau kealpaan sebagai bentuk kesalahan. Sistem AI yang menghasilkan rekayasa suara, wajah, maupun video tidak dapat ditempatkan sebagai subjek pertanggungjawaban pidana hanya berdasarkan kemampuannya menghasilkan konten sintetis. Perbuatan tersebut harus dikaitkan dengan manusia yang menginisiasi, mengoperasikan, mengarahkan, mengendalikan, atau memanfaatkan teknologi untuk mencapai tujuan tertentu yang dilarang oleh hukum pidana. Posisi tersebut sejalan dengan kajian mengenai pertanggungjawaban pidana atas penyalahgunaan *deepfake* yang menempatkan AI sebagai instrumen dan mengarahkan pertanggungjawaban kepada pihak yang menciptakan, memerintahkan, menyebarkan, mengendalikan, atau memperoleh manfaat dari penggunaannya. Hubungan antara kehendak manusia dan penggunaan teknologi menjadi penting untuk menentukan pertanggungjawaban, khususnya ketika *deepfake* digunakan sebagai sarana untuk membangun keyakinan palsu pada korban agar menyerahkan uang, barang, atau keuntungan sebagaimana menjadi bagian dari konstruksi penipuan menurut Pasal 492 KUHP Nasional.

Pembagian pertanggungjawaban juga harus memperhatikan kontribusi konkret setiap pihak terhadap terlaksananya penipuan. Pembuat konten *deepfake* yang sejak awal mengetahui tujuan penggunaan hasil rekayasa tersebut dan secara sadar menyediakan konten untuk mendukung penipuan dapat ditempatkan sebagai pihak yang bertanggung jawab secara pidana sesuai dengan bentuk keterlibatannya. Posisi serupa berlaku terhadap pihak yang menggunakan konten *deepfake* untuk menyamarkan identitas dan secara langsung membujuk korban agar menyerahkan uang atau barang, karena pihak tersebut memiliki hubungan yang erat dengan pelaksanaan delik penipuan. Kerja sama yang dilakukan secara sadar dan diarahkan pada terwujudnya tindak pidana dapat dikualifikasikan sebagai turut serta melakukan (*medeplegen*) sebagaimana Pasal 20 huruf c KUHP Nasional apabila unsur kerja sama dan kontribusi masing-masing pihak dapat dibuktikan. Berbeda dari turut serta, pihak yang dengan sengaja memberikan kesempatan, sarana, atau keterangan, ataupun memberikan bantuan ketika tindak pidana dilaksanakan, dapat ditempatkan sebagai pembantu (*medeplichtigheid*) berdasarkan Pasal 21 KUHP Nasional. Oleh sebab itu, status pembuat *deepfake* tidak dapat ditentukan hanya berdasarkan fakta bahwa ia menghasilkan konten sintetis, tetapi perlu dilihat dari pengetahuan, kehendak, tujuan, serta bentuk kontribusinya terhadap tindak pidana yang kemudian dilakukan.

Permasalahan pertanggungjawaban menjadi berbeda ketika pembuat *deepfake* tidak mengetahui bahwa konten yang dihasilkannya akan digunakan sebagai sarana penipuan. Pemenuhan aspek perbuatan pidana tidak serta-merta cukup untuk membebankan pertanggungjawaban kepada orang tersebut karena KUHP Nasional mensyaratkan adanya kesalahan berupa kesengajaan atau kealpaan. Kealpaan pun hanya dapat menjadi dasar pemidanaan apabila bentuk tindak pidana tersebut secara tegas ditentukan oleh peraturan perundang-undangan. Penjelasan Pasal 36 menempatkan ketentuan tersebut sebagai perwujudan prinsip *geen straf zonder schuld*, yaitu tiada pidana tanpa kesalahan.⁴ Konsekuensinya, penyedia perangkat lunak, operator teknologi, pembuat konten, ataupun pihak lain yang memiliki hubungan dengan teknologi *deepfake* tidak dapat dipidana hanya karena produk atau teknologi yang digunakan olehnya kemudian disalahgunakan oleh orang lain. Pertanggungjawaban terhadap pihak tersebut memerlukan pembuktian mengenai kesengajaan atau bentuk kesalahan lain yang diakui hukum pidana, termasuk pengetahuan mengenai tujuan kriminal serta adanya kontribusi yang diberikan secara sadar terhadap pelaksanaan penipuan. Pembatasan tersebut diperlukan agar penerapan hukum pidana tetap membedakan penggunaan teknologi untuk kepentingan yang sah dari penggunaan teknologi yang sejak awal diarahkan untuk melakukan tindak pidana.⁵

Konstruksi tersebut menunjukkan perlunya penentuan pertanggungjawaban berdasarkan peran masing-masing pihak (*role-based criminal liability*), bukan dengan memberikan status pidana yang sama kepada seluruh orang yang memiliki hubungan dengan teknologi *deepfake*. Pihak yang mengendalikan skema penipuan dan menggunakan *deepfake* secara langsung untuk membentuk keyakinan palsu pada korban dapat ditempatkan sebagai pelaku. Pihak yang secara sadar melakukan kerja sama dan memberikan kontribusi terhadap pelaksanaan penipuan dapat dinilai melalui konstruksi turut serta, sedangkan pihak yang memberikan sarana, kesempatan, atau keterangan secara sengaja dapat dinilai berdasarkan ketentuan pembantuan apabila persyaratan Pasal 21 terpenuhi. Pembagian tersebut berkaitan dengan prinsip kebijakan hukum pidana yang menempatkan kesalahan dan proporsionalitas sebagai dasar penting dalam menentukan dapat atau tidaknya seseorang dibebani pertanggungjawaban pidana.⁶ Kebutuhan untuk membedakan peran tersebut juga terlihat dari kajian mengenai penyalahgunaan *deepfake* yang menunjukkan adanya persoalan normatif dalam menentukan *actus reus*, *mens rea*, serta batas pertanggungjawaban pidana pihak-pihak yang terlibat dalam penggunaan teknologi tersebut.⁷ Persoalan tersebut perlu ditempatkan secara hati-hati agar kesenjangan pengaturan mengenai AI tidak mendorong penafsiran Pasal 492 secara analogis terhadap setiap orang yang memiliki hubungan dengan teknologi *deepfake*, sementara konstruksi penyertaan dan pembantuan dalam KUHP Nasional masih dapat digunakan untuk menguji bentuk kontribusi masing-masing pihak.

Penerapan konstruksi tersebut dapat dilakukan secara bertahap dengan menghubungkan pembuktian tindak pidana, kedudukan pihak yang terlibat, dan unsur kesalahan sebagai satu rangkaian analisis. Tahap pertama berkaitan dengan pembuktian terpenuhinya unsur penipuan sebagaimana Pasal 492 KUHP Nasional. Setelah perbuatan pidana tersebut dapat diidentifikasi, tahap berikutnya diarahkan pada penentuan posisi setiap pihak berdasarkan bentuk penyertaan sebagaimana Pasal 20 dan pembantuan sebagaimana Pasal 21. Penilaian tersebut kemudian harus disertai pembuktian mengenai kesalahan berdasarkan Pasal 36 serta pemeriksaan terhadap

kemungkinan adanya alasan pembenar atau alasan pemaaf yang memengaruhi pertanggungjawaban pidana. Struktur semacam ini memungkinkan *deepfake* diposisikan sebagai sarana yang digunakan untuk melaksanakan tindak pidana, sedangkan subjek yang dimintai pertanggungjawaban tetap merupakan manusia yang memiliki hubungan kehendak dan kesalahan dengan perbuatan tersebut. Kebutuhan untuk memperjelas batas pertanggungjawaban setiap pihak tetap terbuka seiring berkembangnya penggunaan AI, terutama ketika hubungan antara pencipta teknologi, pengendali sistem, penyedia sarana, pembuat konten, dan pengguna akhir semakin sulit dipisahkan secara sederhana.

SIMPULAN

Modus penipuan yang memanfaatkan teknologi *deepfake* dapat ditempatkan sebagai tindak pidana penipuan berdasarkan Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana sepanjang unsur-unsur deliknya terpenuhi dan dapat dibuktikan. Manipulasi terhadap wajah, suara, atau video melalui teknologi *deepfake* dapat berfungsi sebagai sarana *tipu muslihat* apabila penggunaannya menciptakan keadaan palsu yang mampu menyesatkan korban dan mendorong korban untuk menyerahkan Barang, memberikan utang, membuat pengakuan utang, atau menghapus piutang. Penggunaan teknologi tersebut tidak serta-merta melahirkan kualifikasi delik yang baru, melainkan merupakan perkembangan cara atau sarana yang digunakan untuk mewujudkan perbuatan penipuan yang telah dirumuskan oleh hukum pidana. Penafsiran terhadap Pasal 492 tetap harus ditempatkan dalam batas asas legalitas dan larangan penggunaan analogi sebagaimana Pasal 1 ayat (2) KUHP Nasional. Batas tersebut diperlukan agar perkembangan teknologi hanya memengaruhi cara pelaksanaan perbuatan, tanpa mengubah atau memperluas norma pidana melebihi cakupan makna yang dapat dibenarkan berdasarkan ketentuan yang berlaku.

Pertanggungjawaban pidana atas penipuan yang menggunakan *deepfake* perlu ditentukan dengan melihat hubungan antara peran, kontribusi, dan kesalahan setiap pihak yang terlibat. Sistem kecerdasan buatan yang digunakan untuk menghasilkan konten *deepfake* tidak ditempatkan sebagai subjek pertanggungjawaban pidana, melainkan sebagai instrumen yang digunakan untuk melaksanakan tindak pidana. Subjek yang dapat dimintai pertanggungjawaban tetap diarahkan kepada manusia yang mempunyai hubungan kesalahan dengan perbuatan tersebut. Pihak yang menggunakan *deepfake* secara langsung sebagai sarana melakukan penipuan dapat diposisikan sebagai pelaku, sedangkan pihak yang secara sadar melakukan kerja sama untuk mewujudkan tindak pidana dapat ditempatkan sebagai pihak yang turut serta berdasarkan Pasal 20 KUHP Nasional. Pihak yang dengan sengaja memberikan kesempatan, sarana, atau keterangan, termasuk bantuan ketika tindak pidana berlangsung, dapat dipertanggungjawabkan berdasarkan Pasal 21 KUHP Nasional apabila unsur pembantuan terpenuhi. Penentuan pertanggungjawaban tersebut tetap mensyaratkan kesalahan sebagaimana Pasal 36 KUHP Nasional. Artinya, pembuat konten, penyedia teknologi, operator, ataupun pihak lain yang berkaitan dengan penggunaan *deepfake* tidak dapat dibebani pidana hanya karena teknologi tersebut kemudian digunakan untuk melakukan penipuan tanpa adanya kesengajaan atau kealpaan yang dapat dipertanggungjawabkan secara pidana. Konstruksi ini menempatkan ketentuan mengenai penipuan, penyertaan, pembantuan, dan kesalahan sebagai dasar untuk menentukan pertanggungjawaban pidana terhadap penipuan berbasis *deepfake*, sementara perkembangan teknologi kecerdasan buatan menunjukkan

perlunya batas pertanggungjawaban yang lebih terukur bagi setiap pihak yang memiliki keterlibatan dalam penggunaannya.

DAFTAR PUSTAKA

- Hiariej, Eddy O. S. *Prinsip-Prinsip Hukum Pidana: Edisi Penyesuaian KUHP Nasional*. Depok: Rajawali Pers, 2024.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Edisi revisi. Jakarta: Kencana, 2017.
- Nawawi Arief, Barda. *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*. Edisi ke-7. Jakarta: Kencana Prenada Media Group, 2011.
- Soekanto, Soerjono, and Sri Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Pers, 2001.
- Syahputra, Novrian, et al. *Hukum Pidana Indonesia: Konsep, Sistem, dan Pembaruan*. Padang: CV Gita Lentera, 2026.
- Syamsudin, Rahman. *Delik-Delik di dalam KUHP*. Jakarta: Kencana, 2025.
- Gunawan, Gunawan. "Limitasi Normatif Pertanggungjawaban Pidana atas Penyalahgunaan *Deepfake* Berbasis Artificial Intelligence di Indonesia." *Jurnal Ilmu Hukum, Humaniora dan Politik* 6, no. 5 (2026): 3929–3936. <https://doi.org/10.38035/jihhp.v6i5.9050>.
- Haq, Zaenul. "Perlindungan Konsumen terhadap Ancaman *Deepfake* dalam Transaksi Digital: Tinjauan Regulasi dan Urgensi Mitigasi." *Journal of Authentic Research* 4, no. 2 (2025): 2656–2669. <https://doi.org/10.36312/m4xwcw14>.
- Indriawati, Sri Endah. "Konstruksi Pertanggungjawaban Pidana atas Pemanfaatan Kecerdasan Buatan dalam Tindak Pidana Berbasis *Deepfake*." *Judge: Jurnal Hukum* 6, no. 10 (2026): 1933–1943. <https://doi.org/10.54209/judge.v6i10.2295>.
- Judijanto, Loso, Andrew Shandy Utama, and Heri Setiyawan. "Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (*Deepfake*) in Indonesia." *The Easta Journal Law and Human Rights* 3, no. 2 (2025): 101–109. <https://doi.org/10.58812/eslhr.v3i02.470>.
- Laza, Jeremiah Maximillian, and Rizky Karo Karo. "Perlindungan Hukum terhadap Artificial Intelligence dalam Aspek Penyalahgunaan *Deepfake Technology* pada Perspektif UU PDP dan GDPR." *LEX PROSPICIT* 1, no. 2 (2023): 136–150. <https://doi.org/10.19166/lp.v1i2.7368>.
- Prayoga, Hendra, and Hadi Tuasikal. "Penyebaran Konten *Deepfake* sebagai Tindak Pidana: Analisis Kritis terhadap Penegakan Hukum dan Perlindungan Publik di Indonesia." *Abdurrauf Law and Sharia* 2, no. 1 (2025): 22–38. <https://doi.org/10.70742/arlash.v2i1.194>.
- Rochman, M. "Criminal Liability for Deepfake Cybercrime: Evidentiary Challenges and Regulatory Gaps in Indonesian Law." *Jurnal Akta* 13, no. 1 (2026): 557–569. <https://doi.org/10.30659/akta.v13i1.49241>.
- Triawan, Agung, Sunardi Purwanda, Muhammad Darwis, Kairuddin, and Bakhtiar Tijjang. "Dinamika Penegakan Hukum terhadap Tindak Pidana Penipuan Perspektif Yuridis." *Innovative: Journal of Social Science Research* 5, no. 4 (2025): 3896–3911. <https://doi.org/10.31004/innovative.v5i4.20678>
- Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Indonesia. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1. Tambahan Lembaran Negara Republik Indonesia Nomor 6842.
- Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

- Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Sari, Rita Puspita. “Apa Itu *Deepfake*? Kenali Bahaya dan Cara Mendeteksinya.” *Cloud Computing Indonesia*. Accessed August 30, 2026. <https://www.cloudcomputing.id/pengetahuan-dasar/apa-itu-deepfake-bahaya>.