INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 11, Tahun 2026, Hal. 47-55, ISSN: 3123-5573 (Online)

Tinjauan Yuridis Tindak Pidana Penipuan Melalui Rekayasa Kecerdasan Bauatan (*Deepfake*)

Marisa Maziah Rahmania[1], Yudhia Ismail[2], Wiwin Ariesta[3]
[1,2,3]Universitas Merdeka Pasuruan
maziahrahmania2@gmail.com[1], yudhiaismail@unmerpas.ac.id[2], wiwinariesta@unmerpas.ac.id[3]

Article Info

Article history:
Received June 25, 2026
Revised July 18, 2026
Accepted July 26, 2026

Keywords:
Deepfake, Fraud, Personal Data Protection, *Criminal Liability*, *Artificial Intelligence*.

ABSTRACT

The rapid advancement of *artificial intelligence* (AI) technology has given rise to a new mode of *cybercrime*: fraud based on *deepfake* technology. *Deepfake* technology utilizes *deep learning* techniques to manipulate or synthesize audiovisual data—such as faces and voices—producing highly realistic digital content. This crime has evolved into a sophisticated form of *social engineering* that exploits victim trust, resulting in material losses and a loss of control over digital identities. This phenomenon demonstrates that the criminal use of biometric data manipulation requires serious attention within the framework of national criminal law enforcement. This study employs a normative-juridical method, utilizing statutory and *conceptual approach*es to examine the Personal Data Protection (PDP) Law, the Electronic Information and Transactions (ITE) Law, and the National Criminal Code. The findings indicate that the unauthorized manipulation of voices or faces using *deepfake*s constitutes a form of creating or falsifying personal data, as regulated in Article 66 in conjunction with Article 68 of the PDP Law. This provision serves as *lex specialis*, complementing the general fraud provisions in the National Criminal Code and the regulations regarding the authenticity of electronic documents in the ITE Law. However, the formulation of Article 66 of the PDP Law remains broad and does not explicitly address *artificial intelligence* tools, potentially creating normative ambiguity and legal loopholes. *Criminal liability* is imposed fully on individual perpetrators when the elements of an unlawful act, capacity for liability, and intent (*mens rea*) are met. *Criminal liability* may also be imposed on a corporation if the crime is committed by, for, or on behalf of the business entity.

Article Info

Article history:
Received June 25, 2026
Revised July 18, 2026
Accepted July 26, 2026

Kata kunci:
Deepfake, Penipuan, Pelindungan Data Pribadi, Pertanggungjawaban Pidana, Kecerdasan Buatan.

ABSTRAK

Perkembangan teknologi kecerdasan buatan (*artificial intelligence*) yang sangat pesat melahirkan modus kejahatan siber baru berupa penipuan berbasis teknologi *deepfake*. Teknologi *deepfake* bekerja dengan memanfaatkan teknik *deep learning* untuk memanipulasi maupun mensintesis data audio visual, seperti wajah dan suara, sehingga menghasilkan konten digital yang tampak sangat realistis. Kejahatan ini bertransformasi menjadi bentuk *social engineering* tingkat lanjut yang menembus kewaspadaan korban dan menimbulkan kerugian materiil serta hilangnya kendali atas identitas digital. Fenomena tersebut menunjukkan bahwa manipulasi data biometrik untuk sarana kejahatan memerlukan perhatian serius dalam kerangka penegakan hukum pidana nasional. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan konseptual, menelaah Undang-Undang Pelindungan Data Pribadi, Undang-Undang Informasi dan Transaksi Elektronik, dan Kitab

Undang-Undang Hukum Pidana Nasional. Hasil penelitian menunjukkan bahwa perbuatan manipulasi suara atau wajah menggunakan *deepfake* tanpa hak pada dasarnya merupakan bentuk pembuatan atau pemalsuan data pribadi yang diatur dalam Pasal 66 jo. Pasal 68 UU PDP. Ketentuan ini berkedudukan sebagai *lex specialis* yang melengkapi aturan penipuan umum pada KUHP Nasional dan keotentikan dokumen elektronik dalam UU ITE. Namun demikian, rumusan Pasal 66 UU PDP masih bersifat umum dan belum secara eksplisit mengatur sarana kecerdasan buatan, sehingga berpotensi menimbulkan kekosongan norma serta ketidakpastian hukum. Pertanggungjawaban pidana dibebankan secara penuh kepada pelaku perorangan apabila terpenuhi unsur perbuatan melawan hukum, kemampuan bertanggung jawab, dan kesengajaan (*mens rea*). Pertanggungjawaban pidana juga dapat diperluas kepada korporasi apabila kejahatan dilakukan oleh, untuk, atau atas nama badan usaha.

Corresponding Author:
Marisa Maziah Rahmania
Universitas Merdeka Pasuruan
Email: maziahrahmania2@gmail.com

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi pada abad ke-21 telah membawa perubahan fundamental dalam berbagai aspek kehidupan manusia. Perkembangan teknologi informasi dan komunikasi menyebabkan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan yang berlangsung sangat cepat. Di satu sisi, akselerasi ini membawa kemajuan pesat, namun di sisi lain, fenomena ini memicu kemunculan modus-modus kejahatan baru di dunia maya (*cybercrime*) yang kian kompleks. Revolusi industri 4.0 yang ditandai oleh kemunculan kecerdasan buatan (*artificial intelligence*/AI), *big data*, dan komputasi awan telah mengubah cara manusia berinteraksi, bertransaksi, dan berkomunikasi secara masif. Fenomena global menunjukkan bahwa penggunaan AI sering kali menimbulkan implikasi etis dan sosial yang rumit. Algoritma yang dirancang untuk mendukung efisiensi terkadang menghasilkan bias diskriminatif, baik secara rasial, gender, maupun status sosial. Menurut Klaus Schwab, revolusi ini tidak sekadar memperluas dan memperdalam jangkauan revolusi digital, melainkan mewakili transformasi cara hidup, bekerja, dan berhubungan antarsesama manusia yang belum pernah terjadi sebelumnya. Di satu sisi, perkembangan tersebut membawa manfaat nyata bagi peningkatan efisiensi dan produktivitas; namun di sisi lain, ia membuka celah eksploitasi baru yang sebelumnya tidak terbayangkan dalam kerangka hukum konvensional.

Salah satu produk paling revolusioner sekaligus paling berbahaya dari kecerdasan buatan adalah teknologi *deepfake*, sebuah teknik sintesis media berbasis algoritma *deep learning* yang mampu menciptakan konten audio, visual, maupun audiovisual palsu yang tampak sangat meyakinkan. Teknologi ini pertama kali diperkenalkan secara ilmiah melalui penelitian Suwajanakorn dkk., yang berhasil mensintesis video *lip-sync* secara sangat akurat. Pada tahun 2023, masyarakat Indonesia dihebohkan dengan beredarnya sebuah video yang menampilkan Presiden Joko Widodo (Jokowi) berpidato dengan lancar dalam bahasa Mandarin. Video ini dengan cepat menyebar di berbagai platform media sosial, memicu kebingungan dan spekulasi di kalangan publik. Karena semakin maraknya

penyebaran video tersebut, Kementerian Komunikasi dan Informatika (Kominfo) segera turun tangan dan mengonfirmasi bahwa video tersebut merupakan hasil manipulasi *deepfake*. Meskipun telah diklarifikasi, dampaknya tidak bisa dianggap remeh, membuktikan betapa akuratnya manipulasi digital yang dapat dihasilkan mesin. Dalam waktu singkat, teknologi yang semula terbatas pada riset akademik tersebut bermigrasi ke ranah publik dan kini dapat diakses secara bebas melalui berbagai aplikasi daring komersial.

Dalam konteks kejahatan siber, *deepfake* telah berevolusi menjadi instrumen penipuan yang canggih dan sulit dideteksi. Laporan Deeptrace Labs mengungkapkan bahwa pada tahun 2019 saja telah beredar lebih dari

14.000 video *deepfake* daring dan angka tersebut tumbuh secara eksponensial setiap tahunnya. Lebih mengkhawatirkan adalah pergeseran orientasi penggunaannya. Jika semula *deepfake* banyak dimanfaatkan untuk manipulasi konten hiburan, kini semakin banyak digunakan untuk penipuan finansial, penyebaran disinformasi, serta pemerasan berbasis konten seksual palsu. Di antara berbagai varian *deepfake*, *deepfake* audio atau kloning suara (*voice cloning*) muncul sebagai ancaman paling serius dalam dimensi penipuan finansial. Teknologi ini bekerja dengan merekayasa karakteristik unik suara seseorang meliputi intonasi, ritme, aksen, dan pola bicara melalui pemrosesan sampel suara yang sangat singkat, bahkan hanya dari beberapa detik rekaman. Suara sintesis yang dihasilkan kemudian digunakan pelaku untuk menyamar sebagai pejabat perusahaan, anggota keluarga, atau tokoh otoritas guna memperoleh transfer dana, informasi rahasia, maupun tindakan tertentu dari korban.

Dalam konteks kejahatan siber, *deepfake* telah berevolusi menjadi instrumen penipuan yang canggih dan sulit dideteksi. Laporan Deeptrace Labs mengungkapkan bahwa pada tahun 2019 saja telah beredar lebih dari

14.000 video *deepfake* daring dan angka tersebut tumbuh secara eksponensial setiap tahunnya. Lebih mengkhawatirkan adalah pergeseran orientasi penggunaannya. Jika semula *deepfake* banyak dimanfaatkan untuk manipulasi konten hiburan, kini semakin banyak digunakan untuk penipuan finansial, penyebaran disinformasi, serta pemerasan berbasis konten seksual palsu. Di antara berbagai varian *deepfake*, *deepfake* audio atau kloning suara (*voice cloning*) muncul sebagai ancaman paling serius dalam dimensi penipuan finansial. Teknologi ini bekerja dengan merekayasa karakteristik unik suara seseorang meliputi intonasi, ritme, aksen, dan pola bicara melalui pemrosesan sampel suara yang sangat singkat, bahkan hanya dari beberapa detik rekaman. Suara sintesis yang dihasilkan kemudian digunakan pelaku untuk menyamar sebagai pejabat perusahaan, anggota keluarga, atau tokoh otoritas guna memperoleh transfer dana, informasi rahasia, maupun tindakan tertentu dari korban.

Fenomena penipuan berbasis *deepfake* audio ini sangat relevan dengan realitas empiris dan pengalaman empiris di lapangan. Sebagaimana kasus konkret di mana korban menerima pesan melalui aplikasi WhatsApp dari seseorang yang menggunakan foto profil dan identitas menyerupai kerabat dekat korban. Dalam percakapan tersebut, pelaku menghubungi korban dengan bahasa yang sangat meyakinkan. Pelaku kemudian menyampaikan bahwa dirinya sedang berada dalam keadaan mendesak dan membutuhkan bantuan dana sebesar Rp 3.000.000,- untuk keperluan darurat. Karena identitas dan foto yang digunakan tampak nyata, korban tidak langsung menaruh curiga.

Tidak hanya menggunakan identitas dan foto yang menyerupai kerabat korban, pelaku juga mengirimkan pesan suara (*voice note*) dengan suara yang terdengar identik dengan suara asli kerabat korban. Suara tersebut digunakan pelaku untuk semakin meyakinkan korban agar percaya bahwa orang yang sedang menghubunginya benar-benar anggota keluarga sendiri. Dalam pesan suara itu, pelaku meminta bantuan dengan nada panik dan terburu-buru sehingga korban merasa iba dan tergerak untuk mentransfer dana. Penggunaan suara asli tersebut merupakan hasil rekayasa teknologi kecerdasan buatan atau *deepfake* audio yang meniru karakteristik suara seseorang secara detail dari sampel suara digital yang diunduh dari media sosial terbuka. Setelah dana ditransfer, komunikasi terputus dan nomor

pelaku tidak aktif. Kasus semacam ini menimbulkan kerugian materiil serta dampak psikologis berupa trauma, rasa takut, dan hilangnya kepercayaan terhadap media komunikasi digital. Modus penggunaan suara palsu yang menyerupai suara asli korban menjadi salah satu bentuk kejahatan siber modern yang sangat sulit dikenali oleh masyarakat awam karena pelaku mampu menciptakan komunikasi yang tampak sangat nyata.

Indonesia tidak terlepas dari ancaman kejahatan siber berbasis AI ini. Data Bareskrim Polri menunjukkan peningkatan laporan penipuan berbasis teknologi sebesar 40% pada tahun 2023 dibandingkan tahun sebelumnya, dengan modus operandi yang semakin beragam dan sulit dilacak. Salah satu kasus yang mencuat adalah penipuan menggunakan suara kloning seorang direktur bank yang berhasil mengelabui staf keuangan perusahaan hingga mengakibatkan kerugian sebesar Rp 3,2 miliar. Secara global, FBI melaporkan bahwa penipuan melalui *Business Email Compromise* (BEC) yang kini telah berevolusi menggunakan *deepfake* audio menyebabkan kerugian lebih dari USD 2,9 miliar pada tahun 2023. Kasus serupa terjadi di Eropa, di mana seorang direktur eksekutif perusahaan energi di Inggris mentransfer sekitar USD 243.000 setelah menerima perintah via telepon dari suara palsu yang menyerupai suara CEO perusahaan induknya di Jerman, menjadikannya salah satu kasus *deepfake* audio korporasi yang terdokumentasi dengan jelas. Fakta-fakta ini mempertegas bahwa *deepfake* audio bukan sekadar ancaman hipotetis, melainkan modus kejahatan nyata yang telah beroperasi dan menimbulkan kerugian konkret.

Meskipun ancaman *deepfake* audio telah nyata terjadi, respons hukum Indonesia terhadap fenomena ini masih berada dalam kondisi yang belum memadai (*legal gap*). Selama ini, penuntutan atas tindak pidana penipuan berbasis *deepfake* umumnya mengandalkan ketentuan umum, yakni Pasal 492 Kitab Undang-Undang Hukum Pidana (KUHP Nasional / UU No. 1 Tahun 2023) tentang tindak pidana perbuatan curang 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."

Selain itu, penuntut umum juga sering mengaitkan dengan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang berbunyi: Setiap Orang yang dengan sengaja menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah)."

Kedua ketentuan di atas tidak secara eksplisit mengatur penggunaan kecerdasan buatan sebagai sarana penipuan, sehingga penerapannya terhadap kasus *deepfake* audio mengandung kelemahan konstruktif yang dapat dieksploitasi oleh pihak terdakwa. Di sisi lain, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) hadir sebagai instrumen hukum baru yang sangat potensial namun belum banyak dieksplorasi dalam konteks penipuan berbasis *deepfake*. Secara khusus, Pasal 68 jo. Pasal 66 UU PDP mengatur sanksi pidana terhadap pihak yang memalsukan data pribadi. Pasal 66 UU PDP menegaskan:

Setiap Orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain." Ancaman pidana atas perbuatan tersebut diatur dalam Pasal 68 UU PDP, yaitu :

Setiap Orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain sebagaimana dimaksud dalam Pasal 66 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp 6.000.000.000,00 (enam miliar rupiah)."

METODE

Penelitian ini merupakan penelitian hukum normatif (*juridical normative research*), yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan kepustakaan atau data sekunder. Menurut Peter Mahmud Marzuki, penelitian hukum adalah suatu proses untuk menemukan aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi. Pendekatan penelitian yang digunakan mencakup: Pendekatan Perundang-undangan (*Statute Approach*): Menganalisis secara mendalam berbagai peraturan perundang-undangan yang relevan, yaitu KUHP Nasional (UU No. 1 Tahun 2023), UU Pelindungan Data Pribadi (UU No. 27 Tahun 2022), dan UU Informasi dan Transaksi Elektronik (UU No. 11 Tahun 2008 jo. UU No. 1 Tahun 2024). Pendekatan Konseptual (*Conceptual Approach*): Merujuk pada konsep-konsep, doktrin, dan prinsip-prinsip hukum pidana mengenai pertanggungjawaban pidana, asas *lex specialis derogat legi generali*, serta doktrin pelindungan data pribadi dan hukum siber.

Data yang digunakan adalah data sekunder yang terdiri dari tiga bahan hukum: Bahan Hukum Primer: Kitab Undang-Undang Hukum Pidana (KUHP Nasional / UU No. 1 Tahun 2023). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). 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 (UU ITE). Bahan Hukum Sekunder: Buku-buku teks hukum pidana, hukum siber, dan AI (karya Peter Mahmud Marzuki, Eddy O.S. Hiariej, Edmon Makarim, Stuart Russell, Klaus Schwab, dll.). Jurnal-jurnal hukum nasional dan internasional yang terakreditasi mengenai *deepfake*, *cybercrime*, dan pelindungan data pribadi. Bahan Hukum Tersier: Kamus Besar Bahasa Indonesia (KBBI), Kamus Hukum, dan ensiklopedia yang memberikan petunjuk atau penjelasan atas bahan hukum primer dan sekunder. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan melakukan inventarisasi, pencatatan, dan pengkatalogan bahan hukum. Analisis bahan hukum dilakukan secara kualitatif deduktif, yaitu menarik kesimpulan dari prinsip-prinsip umum hukum pidana dan norma undang-undang untuk diterapkan pada fenomena konkret tindak pidana penipuan berbasis *deepfake*. Penafsiran hukum yang digunakan meliputi penafsiran gramatikal, sistematis, dan teleologis.

HASIL DAN PEMBAHASAN

a. Pengaturan Tindak Pidana Penipuan yang Menggunakan Teknologi Kecerdasan Buatan (*Deepfake*) Berdasarkan Pasal 66 Undang-Undang Pelindungan Data Pribadi

Perkembangan teknologi kecerdasan buatan telah melahirkan dimensi kejahatan siber yang semakin dinamis. Salah satu manifestasi paling nyata dari penyalahgunaan AI adalah penggunaan teknologi *deepfake* untuk melancarkan tindak pidana penipuan. Karakteristik utama *deepfake* terletak pada kemampuannya mereplikasi identitas biometrik seseorang berupa wajah dan suara secara sangat presisi. Ketika identitas biometrik ini diekstrak, diolah, dan direkayasa tanpa izin subjek data untuk mengelabui korban demi memperoleh keuntungan finansial, perbuatan tersebut secara substantif telah memasuki ranah kejahatan pemalsuan data pribadi.

Konstruksi Yuridis Pasal 66 UU Pelindungan Data Pribadi Sesuai dengan ketentuan Pasal 1 angka 1 UU PDP, Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya. Selanjutnya, Pasal 4 ayat (2)

UU PDP mengategorikan data biometrik sebagai Data Pribadi yang Bersifat Spesifik. Suara dan visual wajah seseorang merupakan data biometrik yang unik dan melekat secara intrinsik pada harkat martabat individu. Pasal 66 UU PDP merumuskan norma larangan sebagai berikut: “Setiap Orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain."

Sanksi pidana atas pelanggaran Pasal 66 ini diatur dalam Pasal 68 UU PDP, dengan ancaman pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp 6.000.000.000,00 (sebab dalam perubahannya mencakup ancaman denda yang sangat berat). Apabila dianalisis secara gramatikal dan kontekstual, pembuatan konten *deepfake* (baik berupa kloning suara maupun rekonstruksi wajah) menggunakan perangkat lunak AI tanpa hak memenuhi dua perbuatan inti (*actus reus*) dalam Pasal 66 UU PDP: Perbuatan "Membuat Data Pribadi Palsu": Pelaku mengumpulkan sampel suara atau foto korban, kemudian menggunakan model AI untuk menghasilkan audio atau video sintetis baru yang tidak pernah diucapkan atau dilakukan oleh korban asli. Hasil sintesis tersebut merupakan data biometrik tiruan (palsu). Perbuatan "Memalsukan Data Pribadi": Pelaku mengubah atau merekayasa data biometrik yang sudah ada sehingga mengesankan keotentikan, dengan tujuan memperdaya pihak ketiga agar percaya bahwa komunikasi tersebut berasal dari subjek data yang asli.

Hubungan Hukum (*Samenloop*/*Concursus*) Pasal 66 UU PDP dengan KUHP Nasional dan UU ITE. Dalam praktik penegakan hukum, penipuan berbasis *deepfake* sering kali menyentuh beberapa aturan pidana sekaligus. Oleh karena itu, diperlukan pemahaman mendalam mengenai relasi antar-norma hukum pidana yang berlaku di Indonesia: Asas *Lex Specialis Derogat Legi Generali*: Jika dibandingkan dengan Pasal 492 KUHP Nasional (yang merupakan *lex generalis* penipuan), Pasal 66 UU PDP dan Pasal 35 UU ITE berkedudukan sebagai *lex specialis*. Pasal 66 UU PDP secara khusus mengancam pemalsuan data pribadi (biometrik), sedangkan Pasal 35 UU ITE menjangkau tindak manipulasi dokumen elektronik agar dianggap otentik. Konstruksi Perbarengan Pidana (*Concursus Idealismus*): Dalam kasus di mana pelaku menggunakan aplikasi *deepfake* untuk merekayasa suara direktur perusahaan, lalu menyebarkan pesan audio tersebut via WhatsApp untuk menipu staf keuangan hingga menyetor sejumlah uang, perbuatan tunggal tersebut memenuhi unsur dari Pasal 66 UU PDP, Pasal 35 UU ITE, dan Pasal 492 KUHP Nasional secara bersamaan. Penuntut umum dapat mengonstruksikan dakwaan berbentuk kombinasi atau akumulasi (*concursus idealis* - Pasal 50 KUHP Nasional) untuk menjamin keadilan yang menyeluruh.

Kekosongan Yurisprudensi dan Hambatan Kepastian Hukum. Meskipun kerangka normatif telah tersedia, hasil inventarisasi perkara di tingkat peradilan (termasuk penelusuran di Pengadilan Negeri Pasuruan) menunjukkan bahwa belum ada putusan hakim yang secara spesifik mengadili kasus penipuan berbasis *deepfake* audio/video dengan menerapkan Pasal 66 UU PDP. Ketiadaan yurisprudensi ini dipengaruhi oleh beberapa faktor: UU PDP masih berada dalam masa transisi kelembagaan dan sosialisasi sejak disahkan tahun 2022. Aparat penegak hukum lebih cenderung menggunakan pasal-pasal "aman" dan familiar dalam UU ITE (seperti Pasal 28 atau Pasal 35) atau Pasal 378 KUHP lama / Pasal 492 KUHP Nasional. Ketentuan Pasal 66 UU PDP belum secara eksplisit menyebutkan frasa "kecerdasan buatan" atau "sintesis audio-visual", sehingga menimbulkan keraguan penafsir di tingkat penyidikan. Kekosongan yurisprudensi ini berpotensi menimbulkan ketidakpastian hukum (*legal uncertainty*) dan disparitas pemidanaan apabila kasus *deepfake* tidak ditangani dengan standar penafsiran hukum yang seragam. Oleh karena itu, diperlukan terobosan hukum dari hakim (*rechterlijk normstelling*) melalui penafsiran progresif atas Pasal 6UU PDP.

b. Pertanggungjawaban Pidana terhadap Pelaku Tindak Pidana Penipuan yang Memanfaatkan Rekayasa Kecerdasan Buatan (*Deepfake*) Menurut Pasal 66 UU PDP

Pertanggungjawaban pidana (*criminal liability*) adalah meneruskan celaan objektif yang ada pada perbuatan pidana kepada pelaku secara subjektif. Prinsip fundamental yang berlaku adalah *geen straf zonder schuld* (tiada pidana tanpa kesalahan). Dalam kasus penipuan berbasis kecerdasan buatan, penentuan pertanggungjawaban pidana menuntut kejelasan mengenai siapa subjek hukum yang dapat dimintai pertanggungjawaban.

Kecerdasan Buatan sebagai Alat (*Instrumentum Delicti*) dan Posisi Manusia sebagai Subjek Hukum Pidana. Dalam doktrin hukum pidana Indonesia saat ini, kecerdasan buatan (termasuk perangkat lunak *deepfake*) diposisikan sebagai alat (tool/means) dan bukan sebagai subjek hukum pidana. AI tidak memiliki akal budi, kesadaran, kehendak bebas, maupun jiwa (*mens rea*). Oleh sebab itu, AI tidak dapat dijatuhi sanksi pidana. Pertanggungjawaban pidana sepenuhnya dibebankan kepada manusia (*natuurlijke persoon*) yang mengoperasikan, memerintahkan, atau memprogram AI tersebut untuk tujuan kejahatan.

Model pertanggungjawaban pidana dapat dipetakan sebagai berikut: Elemen Pembuktian Pertanggungjawaban Pidana Pelaku Perorangan (Pasal 66 UU PDP): *Actus Reus* (Perbuatan Melawan Hukum): Tindakan merekam, mengunduh, merekayasa data biometrik korban menggunakan aplikasi *deepfake*, dan mengirimkannya kepada sasaran penipuan. *Mens Rea* (Kesengajaan/Maksud): Niat batin pelaku yang diniatkan sejak awal untuk menguntungkan diri sendiri/orang lain secara melawan hukum (*dolus premeditatus*). Kemampuan Bertanggung Jawab: Pelaku berada dalam kondisi kejiwaan sehat, mampu menyadari sifat melawan hukum dari tindakannya, dan mampu mengendalikan kehendaknya. Ketiadaan Alasan Penghapus Pidana: Tidak terdapat alasan pembenar (seperti daya memaksa/*overmacht*) atau alasan pemaaf pada diri pelaku.

Pertanggungjawaban Pidana Korporasi (*Corporate Criminal Liability*) Kejahatan siber modern sering kali dikelola secara terorganisasi oleh sindikat yang berbentuk badan usaha atau korporasi cangkang (*shell companies*). UU PDP secara progresif mengatur pertanggungjawaban pidana korporasi. Berdasarkan Pasal 68 jo. Pasal 70 UU PDP, apabila tindak pidana pemalsuan data pribadi sebagaimana dimaksud dalam Pasal 66 dilakukan oleh, untuk, atau atas nama Korporasi, maka pertanggungjawaban pidana dapat dibebankan kepada: Pengurus atau pengendalinya (*directing mind and will*); Pemberi perintah atau penerima manfaat (*beneficial owner*); Korporasi itu sendiri sebagai badan hukum. Pidana yang dapat dijatuhkan kepada Korporasi meliputi pidana denda (yang dapat dilipatgandakan hingga 3 kali lipat dari maksimum denda perorangan), serta pidana tambahan berupa pencabutan izin usaha, perampasan aset hasil kejahatan, pembekuan seluruh atau sebagian kegiatan usaha, hingga pembubaran korporasi.

Kendala Pembuktian Forensik Digital dan Tantangan Penegakan Hukum. Meskipun norma pertanggungjawaban pidana telah dirumuskan secara tegas, penegakan hukum terhadap kasus penipuan *deepfake* dilapangan menghadapi hambatan teknis yang kompleks: Pembuktian Artefak Digital (*Digital Artifacts*): Konten *deepfake* audio/video berkualitas tinggi sering kali tidak meninggalkan jejak kasat mata. Pembuktian membutuhkan analisis forensik digital tingkat lanjut menggunakan algoritma deteksi frekuensi spektral audio dan pola piksel visual untuk membuktikan bahwa data biometrik tersebut merupakan hasil buatan mesin (sintetis). Anonimitas dan Yuridiksi Lintas Batas (*Borderless* Crime): Pelaku sering kali memanfaatkan jaringan VPN, server terenkripsi di luar negeri, dan sistem pembayaran kripto yang terdesentralisasi, sehingga mengaburkan identitas fisik dan lokasi pelaku (*locus delicti*). Kapasitas Aparat Penegak Hukum: Keterbatasan laboratorium forensik digital yang terspesialisasi dalam deteksi AI di daerah-daerah (seperti Kepolisian Resor) menjadi kendala utama dalam mempercepat proses penyidikan perkara *deepfake*.

KESIMPULAN

Berdasarkan hasil analisis dan pembahasan yang telah diuraikan pada bab-bab sebelumnya, dapat ditarik kesimpulan sebagai berikut: Pengaturan tindak pidana penipuan yang memanfaatkan rekayasa kecerdasan buatan (*deepfake*) dalam sistem hukum Indonesia saat ini belum diatur dalam satu norma tunggal yang eksplisit. Namun secara normatif, perbuatan merekonstruksi atau memalsukan data biometrik berupa wajah dan suara tanpa izin untuk menguntungkan diri sendiri dan merugikan orang lain telah terjangkau oleh Pasal 66 jo. Pasal 68 UU Pelindungan Data Pribadi (UU No. 27 Tahun 2022). Ketentuan ini berkedudukan sebagai *lex specialis* yang melengkapi ketentuan penipuan umum pada Pasal 492 KUHP Nasional dan pemalsuan dokumen elektronik pada Pasal 35 UU ITE. Namun demikian, ketiadaan rincian teknis mengenai kecerdasan buatan dalam rumusan Pasal 66 UU PDP menimbulkan kekosongan norma teknis yang memicu ketidakpastian hukum dalam pembuktian di persidangan.

Pertanggungjawaban pidana terhadap pelaku penipuan berbasis *deepfake* dibebankan secara penuh kepada pelaku perorangan yang mengoperasikan AI apabila terpenuhi unsur *actus reus* (perbuatan melawan hukum), *mens rea* (kesengajaan sebagai maksud/*dolus premeditatus*), dan kemampuan bertanggung jawab. Kecerdasan buatan diposisikan sebagai alat (*instrumentum delicti*) dan bukan subjek hukum. Selain perorangan, pertanggungjawaban pidana juga dapat diperluas kepada Korporasi apabila kejahatan tersebut dilakukan untuk atau atas nama badan usaha. Pembuktian kesalahan pelaku di lapangan masih dihadapkan pada kendala kapasitas forensik digital dan anonimitas teknologi

SARAN

Berdasarkan kesimpulan di atas, penulis mengajukan beberapa saran sebagai berikut: Pembentuk undang-undang perlu mempertimbangkan penyusunan peraturan pelaksana dari UU PDP yang secara eksplisit memberikan definisi dan kualifikasi teknis atas *deepfake* sebagai salah satu bentuk pemalsuan data pribadi, guna memberikan kepastian hukum dan mempermudah penerapan Pasal 66 dalam praktik penegakan hukum. Aparat penegak hukum, khususnya kepolisian dan kejaksaan, perlu ditingkatkan kapasitasnya melalui pelatihan forensik digital dan kerja sama dengan ahli kecerdasan buatan, agar mampu mengumpulkan dan menyajikan alat bukti elektronik secara memadai dalam perkara penipuan berbasis *deepfake*. Diperlukan sinkronisasi dan harmonisasi lebih lanjut antara UU PDP, UU ITE, dan KUHP Nasional melalui pedoman penerapan pasal berlapis (*concursus*), sehingga penegak hukum memiliki acuan yang jelas dalam memilih dan/atau mengombinasikan ketentuan yang paling tepat untuk menjerat pelaku penipuan berbasis *deepfake*. Masyarakat perlu diberikan edukasi dan literasi digital secara berkelanjutan mengenai risiko penyalahgunaan data biometrik dan modus penipuan berbasis *deepfake*, agar dapat lebih berhati-hati dalam menyebarkan data pribadi di ruang digital dan mampu mengenali indikasi konten hasil rekayasa kecerdasan buatan.

DAFTAR PUSTAKA

Buku

Sumarno Hindarto dan Mochamad Alfan Rosid, 2022, Buku Ajar Kecerdasan Buatan/Artificial Intelegent (AI), UMSIDA Press, Sidoarjo;

Tunnel Larry, 2023, *Artificial Intelligence* Basics: A Non-Technical Introduction, CRC Press, Boca Raton;

Deeptrace Lab, 2019, The State of *Deepfakes*: Landscape, Threats and Impact, Deeptrace Labs, Amsterdam;

Europal, 2022, Facing Reality? Law Enforcement and the Challenge of *Deepfake*, Europal Innovation Lab, The Hague;

Komar Mieke Kantaatmadja, et al, 2002, Cyberlaw: Suatu Pengantar, ELIPS II, Bandung;

Peraturan Perundang-Undangan

Kitab Undang-Undang Hukum Pidana Nomor 1 Tahun 2023 (KUHP Nasional)

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Jurnal

Aliya Nur Rasyidah, Urgensi Pembuatan Regulasi Pengguna AI (*Artificial Intelligence*) Di Indonesia, JPHI, Volume. 5, Nomor 1;

Amira Habya Putri, Legal Review of The Use of Personal Data In The Development of Artifial Intelligence Under The Personal Data Protection Law, 2025, Jentera: Jurnal Hukum, Volume. 1, Nomor 1;

Aryitto R.S, Implikasia Hukum *Deepfake*: Telaah terhadap UU ITE dan UU PDP, 2025, Jurnal Ilmiah: Hukum dan Hak Asasi Manusia, Volume. 8, Nomor 2;

Bahiej Ahmad, Kejahatan Penipuan Digital dan Perlindungan Data Pribadi: Tinjauan Yuridis Normatif, 2023, Jurnal Hukum dan Peradilan, Volume. 12, Nomor 1;

Mardiana, Pertanggungjawaban Pidana Korporasi terhadap Pelangnggaran Pelindungan Data Pribadi di Indonesia, 2024, Jurnal Ius Publicum, Volume. 5, Nomor 1;