

TINDAK PIDANA PENIPUAN TEKNOLOGI DEEPPAKE MELALUI MEDIA SOSIAL DALAM PERSPEKTIF HUKUM PIDANA INDONESIA

Aman Wibawa Gintings, S.H., M.H

Program Studi Magister Ilmu Hukum, Fakultas Hukum, Universitas Pasundan, Jawa Barat, Indonesia

**correspondence email: amanwibawagintings@gmail.com*

Prof. Dr. Anthon F. Susanto, S.H., M.Hum

Program Studi Magister Ilmu Hukum, Fakultas Hukum, Universitas Pasundan, Jawa Barat, Indonesia

Abstract: The use of technology to commit fraud is deeply concerning, as technological advancements inevitably lead to increasingly sophisticated methods for perpetrating such crimes – such as the use of Artificial Intelligence (AI), specifically "deepfake" technology, as a tool for fraud. This technological evolution necessitates specific regulations to address the issue. Given these circumstances, the author examines whether existing criminal law provisions are adequate to tackle deepfake-based fraud. To analyze this issue, the study explores two key questions: how deepfake-based fraud via social media is legally constructed under Indonesian criminal law, and how criminal liability is established for perpetrators of such fraud.

This research employs a socio-legal approach, combining legal analysis with social science methodologies. The findings indicate that Indonesian criminal law already possesses a legal basis to address deepfake-based fraud on social media, specifically through Article 492 of the National Criminal Code (KUHP), Article 35 of the Electronic Information and Transactions (ITE) Law, and the Personal Data Protection (PDP) Law. Regarding criminal liability, deepfake-based fraud via social media must satisfy the element of intent (*dolus*); this requires proof that the perpetrator consciously planned the use of deepfake technology, selected the victim's or a public figure's face or digital identity, crafted a fraudulent narrative, and distributed the content across widely accessible social media platforms.

Keywords: *Technology, Deepfake, and Fraud*

Abstrak: Penggunaan teknologi untuk melakukan tindak pidana penipuan tentunya sangat meresahkan mengingat semakin canggihnya teknologi berarti semakin canggih pula pola atau cara yang digunakan untuk melakukan tindak pidana penipuan. Seperti tindak pidana penipuan yang menggunakan Artificial Intelligence (AI) yaitu Deepfake sebagai sarannya. Teknologi yang semakin canggih mendorong pembentukan peraturan khusus yang menanganinya. Dengan karakter yang mendorong diperlukannya suatu pengaturan khusus tersebut, penulis berupaya untuk meninjau lebih lanjut apakah pengaturan hukum pidana yang sudah ada telah memadai dalam penanggulangan tindak pidana penipuan berbasis teknologi Deepfake. Untuk menguraikan permasalahan dalam pengaturan tindak pidana penipuan menggunakan teknologi Deepfake penulis membaginya dengan mendalami beberapa permasalahan terkait dengan Bagaimana konstruksi tindak pidana penipuan berbasis teknologi deepfake melalui media sosial dalam hukum pidana Indonesia dan Bagaimana pertanggungjawaban pidana terhadap pelaku penipuan menggunakan teknologi deepfake melalui media sosial.

Metode pendekatan yang digunakan dalam penelitian ini adalah pendekatan sosio legal, yaitu pendekatan atau penelitian hukum dengan menggunakan metode penelitian menggabungkan analisis hukum dengan pendekatan ilmu sosial. Berdasarkan hasil pembahasan, dapat disimpulkan bahwa hukum pidana Indonesia pada dasarnya telah memiliki landasan yuridis untuk menanggulangi tindak pidana penipuan berbasis teknologi deepfake melalui media sosial, khususnya melalui Pasal 492 KUHP Nasional, Pasal 35 UU ITE, dan UU PDP. Dari sisi pertanggungjawaban pidana, penipuan berbasis teknologi deepfake melalui media sosial harus memenuhi elemen kesengajaan (*dolus*) dimana pelaku secara sadar merencanakan penggunaan teknologi deepfake, memilih wajah atau identitas digital korban atau tokoh publik, menyusun skenario narasi penipuan, dan mendistribusikan konten tersebut melalui platform media sosial yang memiliki jangkauan luas.

Kata Kunci: *Teknologi, Deepfake, dan Penipuan*

A. PENDAHULUAN

Teknologi merupakan hal yang sangat penting di era globalisasi saat ini di mana Teknologi adalah suatu sistem yang dirancang oleh manusia dengan tujuan untuk mempermudah dan menghasilkan tingkat efisiensi dan efektifitas dengan memberikan dampak yang besar tapi dengan tenaga yang sekecil-kecilnya. Teknologi dikembangkan dengan tujuan untuk membantu manusia dalam mempermudah pekerjaannya, dari hal yang remeh sampai hal yang rumit.¹ Perkembangan Teknologi telah mencapai 4.0, di mana pada tahap ini Teknologi berkembang pada penggabungan informasi dan Teknologi cyber (*cyber physical system*).² Dalam perkembangan Teknologi pada tahap ini, bidang informasi mengalami perkembangan yang sangat pesat. Salah satu bentuk perpaduan teknologi dan informasi yang sedang berkembang pesat saat ini adalah artificial intelligence (AI) atau yang dalam Bahasa Indonesia disebut Kecerdasan Buatan.

Perkembangan AI yang pesat terjadi di hampir seluruh bagian dunia, hal ini dikarenakan banyaknya orang yang menggunakan teknologi yang sedang berkembang untuk membantu dan mempermudah pekerjaan manusia sehari-hari. Pesatnya perkembangan AI menimbulkan munculnya sisi positif dan negatif terhadap kehidupan manusia sehari-hari. Sisi positif dari pesatnya perkembangan AI adalah banyaknya pekerjaan manusia yang dapat dipermudah dengan menggunakan teknologi. Dibidang hukum sendiri kegunaan AI dapat membantu proses penegakan hukum, seperti identifikasi pelaku kejahatan, analisis bukti, hingga pengelolaan dokumen hukum.³ Kendati demikian, penggunaan AI dalam bidang hukum juga memiliki potensi penyalahgunaan yaitu penggunaan AI yang dimanfaatkan untuk mempermudah melakukan tindak kriminal atau dikenal dengan sebutan cybercrime.⁴

Teknologi yang awalnya diperuntukkan untuk memudahkan setiap orang untuk dapat berinteraksi dengan cepat, mudah dan murah malah disalahgunakan oleh sebagian orang yang tidak bertanggungjawab untuk melakukan tindak pidana penipuan.⁵ Penggunaan teknologi untuk melakukan tindak pidana penipuan tentunya sangat meresahkan mengingat semakin canggihnya teknologi berarti semakin canggih pula pola atau cara yang digunakan untuk melakukan tindak pidana penipuan. Seperti tindak pidana penipuan yang menggunakan *Artificial Intelligence* (AI) yaitu *Deepfake* sebagai sarannya.⁶

Deepfake merupakan teknologi yang berasal dari AI, yang mana Teknologi deepfake dapat dengan mudah memanipulasi, menukar atau meniru wajah, ekspresi, pola atau mimik, dan suara orang lain, sehingga seakan-akan ekspresi, gerak tubuh, atau suara yang dihasilkan itu terlihat seperti nyata.⁷ *Deepfake* merupakan aplikasi yang dapat diakses oleh semua golongan masyarakat. Mudah akses terhadap aplikasi *Deepfake* mengakibatkan aplikasi ini semakin mudah untuk disalahgunakan, salah satunya untuk melakukan tindak pidana penipuan. Di Indonesia sendiri sudah terjadi beberapa tindak pidana penipuan yang menggunakan aplikasi *Deepfake* seperti yang terjadi di Provinsi Jawa Timur di mana Khofifah sebagai tersangka menggunakan wajah Gubernur Jawa Timur untuk melakukan tindak pidana penipuan. Tersangka telah melakukan tindak pidana penipuan menggunakan aplikasi *Deepfake* yang diunggah pada media sosial Instagram, selama 3 bulan dan telah meraup keuntungan sebesar Rp 87 Juta, dengan korban yang tersebar dari berbagai tempat di Provinsi Jawa Timur.⁸ Contoh lain terjadi di Provinsi Lampung di mana tersangka dengan inisial AMA

¹ Faisal Tamimi, Siti Munawaroh, 2024, "Teknologi Sebagai Kegiatan Manusia Dalam Era Modern Kehidupan Masyarakat", Jurnal Teknologi dan Sistem Informasi, Volume 2, Nomor 3.

² Nabilah Purba, dkk., 2021, "Revolusi Industri 4.0 : Peran Teknologi Dalam Eksistensi Penguasaan Bisnis dan Implementasinya", Jurnal Perilaku dan Strategi Bisnis, Volume 9, Nomor 2.

³ Rendi Septiawan dkk, 2024, "Pemanfaatan Artificial Intelligence dalam Hukum Acara Pidana : Tinjauan Yuridis dan Dampak Sosial", PERKARA Jurnal Ilmu Hukum dan Politik, Volume 2, Nomor 4.

⁴ Ari Ayu Astuti, 2024, "Literasi Kemanfaatan Teknologi Terhadap Kejahatan Terorganisir Lintas Batas Negara di Era Disrupsi dengan AI (Artificial Intelligence)", Indonesian Journal of Criminal Law and Criminology, Volume 5, Nomor 3.

⁵ Silvia Mah Arani Iskandar Putri, dkk, 2024, "Kriminalisasi Penggunaan Deepfake Dalam Tindak Pidana Penipuan Dan Pencemaran Nama Baik : Tantangan Dan Solusi Hukum", Jurnal Hukum Lagalita, Volume 6, Nomor 2.

⁶ *Ibid*

⁷ *Ibid*

⁸ DetikNews.com, "Pelaku Penipuan *Deepfake* Khofifah Raup Untung Rp 87 Juta Selama 3 Bulan",

yang menggunakan wajah Presiden Prabowo Subianto untuk melakukan tindak pidana penipuan. Tersangka telah melakukan tindak pidana penipuan selama 4 bulan dengan meraup keuntungan sebesar Rp 30 Juta, dengan 11 korban yang tersebar di beberapa wilayah di Indonesia yaitu Jawa Tengah, Jawa Timur, Sumatera Selatan, Sumatera Tenggara dan Sulawesi Tengah.⁹

Maraknya kasus penipuan menggunakan aplikasi *Deepfake* menuntut Indonesia agar dapat menanggulangi masalah tindak pidana tersebut. Salah satu cara untuk dapat menanggulangi masalah tersebut adalah melalui ketersediaan regulasi yang memadai.¹⁰ Di Indonesia terdapat Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). Peraturan UU ITE mencakup mengenai Informasi Elektronik, Transaksi Elektronik, Tanda Tangan Elektronik, dan Penyelenggara Sistem Elektronik.¹¹ Dalam UU ITE telah diatur dalam BAB VII tentang Perbuatan yang Dilarang, dimana perbuatan yang dilarang tersebut adalah Peretasan, Pencemaran Nama Baik, Ujaran Kebencian, Konten Ilegal, dan Ancaman Kekerasan. Dalam UU ITE, kasus tindak pidana penipuan melalui aplikasi *Deepfake* dapat dilihat dalam Pasal 35 UU ITE yang berbunyi “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.”

Dengan peraturan yang telah diatur dalam UU ITE, tindakan yang menyangkut tindak pidana penipuan menggunakan aplikasi *Deepfake* dapat dihukum, tetapi tidak ada peraturan dalam UU ITE yang mengatur mengenai tindakan preventif untuk mencegah hal tersebut terus terjadi. Tindakan preventif lebih menekankan pada pencegahan sebelum terjadinya suatu tindak pidana sehingga seharusnya UU ITE dapat mengakomodir pendekatan preventif untuk kejahatan yang bersifat *high tech crime* dengan pendekatan teknologi.¹² Jika ditinjau lebih jauh, pengaturan sebagaimana dimaksud dalam UU ITE tidak mengatur secara khusus mengenai tindak pidana yang memuat langsung unsur dan karakter *Deepfake*. Hal ini juga dapat mengindikasikan terjadinya kekosongan hukum terkait dengan tindak pidana menggunakan teknologi *Deepfake*. Ketidadaan pengaturan khusus terkait kejahatan menggunakan teknologi *Deepfake* beresiko menimbulkan ketidakpastian hukum dan variasi putusan yang menjadikan maraknya kasus tindak pidana penipuan melalui aplikasi *Deepfake*.¹³

Selain mengindikasikan kekosongan hukum, tidak adanya pengaturan tersebut memunculkan suatu pertanyaan terkait dengan konstruksi tindak pidana penipuan melalui media sosial dalam hukum pidana. Apakah konstruksi tindak pidana penipuan melalui media sosial (salah satunya penggunaan teknologi *Deepfake*) memiliki ciri khas atau karakter yang berbeda dengan tindak pidana penipuan konvensional sebagaimana dalam KUHP Nasional.¹⁴ Dalam hal ditemukan bahwa terdapat perbedaan karakter antara tindak pidana penipuan yang menggunakan teknologi *Deepfake* dengan tindak pidana penipuan konvensional, memunculkan pertanyaan lebih lanjut mengenai bagaimana pertanggungjawaban pidana terhadap pelaku tindak pidana yang menggunakan teknologi *Deepfake* di

30 April 2025, https://news.detik.com/berita/d-7892246/pelaku-penipuan-deepfake-khofifah-raup-untung-rp-87-juta-selama-3-bulan?utm_source=chatgpt.com

⁹ Kompas.com, “Video “*Deepfake*” Prabowo Sudah Menelan 11 Korban dalam 4 Bulan Terakhir”,

23 Januari 2025, https://nasional.kompas.com/read/2025/01/23/16382331/video-deepfake-prabowo-sudah-menelan-11-korban-dalam-4-bulan-terakhir?utm_source=chatgpt.com.

¹⁰ Silvia Mah Arani Iskandar Putri, dkk, *Op Cit*

¹¹ Nadella Anggreani, “Pandangan Masyarakat Indonesia tentang UUIITE”, JDIH Kabupaten Tanah Laut, Rabu 7 Mei 2025, https://jdih.tanahlautkab.go.id/artikel_hukum/detail/pandangan-masyarakat-indonesia-tentang-uu-ite/pandangan-masyarakat-indonesia-tentang-uuite#:~:text=1.,jenis%2C%20dan%20prosedur%20transaksi%20elektronik

¹² Noor Rahmad, 2019, “Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online”, J-HES Jurnal Hukum Ekonomi Syariah, Volume 3, Nomor 2.

¹³ Dimas Kresna Prayoga dan Ibrahim Fikma Edrisy, 2025, “Urgensi Pengaturan Hukum Terhadap Deepfake Sebagai Alat Kejahatan Siber Dalam Perspektif KUHP dan UU ITE”, Journal Evidence Of Law, Volume 4, Nomor 3.

¹⁴ Rachman Ma’ruf. Dkk, 2023, “Pengaturan Hukum Tindak Pidana Penipuan Secara Online Dalam Perspektif Hukum Pidana di Indonesia”, Jurnal Hukum dan Sosial Politik, Volume 1, Nomor 2.

media sosial sebagai sarannya. Apakah pertanggungjawaban pidana sebagaimana dalam KUHP Nasional dapat mengakomodir karakteristik pelaku tindak pidana dalam ruang siber.¹⁵

Untuk menguraikan permasalahan dalam pengaturan tindak pidana penipuan menggunakan teknologi *Deepfake* sebagaimana dijelaskan di atas, penulis membaginya dengan mendalami beberapa permasalahan terkait dengan Bagaimana konstruksi tindak pidana penipuan berbasis teknologi *deepfake* melalui media sosial dalam hukum pidana Indonesia dan Bagaimana pertanggungjawaban pidana terhadap pelaku penipuan menggunakan teknologi *deepfake* melalui media sosial. Berdasarkan permasalahan tersebut maka judul penulisan ini adalah “TINDAK PIDANA PENIPUAN TEKNOLOGI DEEPFAKE MELALUI MEDIA SOSIAL DALAM PERSPEKTIF HUKUM PIDANA INDONESIA”.

B. METODE

Metode penelitian adalah prosedur atau cara memperoleh pengetahuan yang benar atau kebenaran melalui Langkah-langkah yang sistematis. Spesifikasi penelitian yang digunakan dalam penelitian ini bersifat deskriptif-analitis. Penelitian deskriptif adalah penelitian dengan metode untuk menggambarkan suatu hasil penelitian. Sesuai dengan namanya, jenis penelitian deskriptif memiliki tujuan untuk memberikan deskripsi, penjelasan, juga validasi mengenai fenomena yang diteliti.¹⁶ Metode pendekatan yang digunakan dalam penelitian ini adalah pendekatan sosio legal, yaitu pendekatan atau penelitian hukum dengan menggunakan metode penelitian menggabungkan analisis hukum dengan pendekatan ilmu sosial.

Metode penelitian sosio-legal melibatkan pengumpulan data empiris melalui berbagai teknik seperti wawancara mendalam, observasi partisipatif, dan analisis dokumen. Data yang dikumpulkan mencakup perilaku manusia baik secara verbal maupun tindakan nyata dalam konteks interaksi sosial. Fokus utama dari penelitian ini adalah fenomena tindak pidana penipuan yang menggunakan *deepfake* (manipulasi digital) sebagai sarannya.¹⁷ Dengan memadukan sumber data empiris dan literatur, diharapkan penelitian ini dapat memberikan gambaran komprehensif mengenai dinamika hukum dan sosial yang melibatkan teknologi *deepfake* (manipulasi digital) dalam melakukan tindak pidana penipuan.

C. HASIL DAN PEMBAHASAN

1. Konstruksi Tindak Pidana Penipuan Berbasis Teknologi Deepfake Melalui Media Sosial Dalam Hukum Pidana Indonesia

Penipuan merupakan salah satu bentuk tindak pidana terhadap harta benda yang secara etimologis berakar dari kata “tipu”, yang menurut Kamus Besar Bahasa Indonesia dimaknai sebagai perbuatan atau perkataan yang tidak jujur—bohong atau palsu—dengan maksud untuk menyesatkan, mengakali, atau mencari keuntungan bagi diri sendiri¹⁸. Secara normatif, perbuatan menipu baru dapat dikategorikan sebagai tindak pidana apabila memenuhi rumusan Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional), yang mulai berlaku efektif sejak 2 Januari 2026. Ketentuan tersebut pada intinya menyatakan bahwa setiap orang yang bermaksud menguntungkan diri sendiri atau orang lain secara melawan

¹⁵ Wahyu Dwi Saputra, Dkk, 2026, “Kajian Terhadap Pertanggungjawaban Pidana Pelaku Kejahatan Siber (Cybercrime) Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik” *Journal of Law, Social Science, And Management Review*, Volume 2, Nomor 3.

¹⁶ Muhammad Ramdhan, 2021, *Metode Penelitian*, Surabaya: Cipta Media Nusantara

¹⁷ Sumarna Dadang dan Ayyub Kadriah, “Penelitian Kualitatif Terhadap Hukum Empiris,” *Jurnal Penelitian Serambi Hukum* 16, no. 02 (2023)

¹⁸ Kamus Besar Bahasa Indonesia (KBBI) Daring, Badan Pengembangan dan Pembinaan Bahasa, Kemendikbudristek, entri “tipu”, diakses 9 Juli 2026.

hukum, dengan memakai nama atau kedudukan palsu, menggunakan tipu muslihat, atau merangkai kata-kata bohong sehingga menggerakkan orang lain untuk menyerahkan suatu barang, memberi utang, membuat pengakuan utang, atau menghapus piutang, diancam dengan pidana penjara paling lama empat tahun atau pidana denda kategori V.

Perbuatan materiil dalam tindak pidana penipuan pada dasarnya adalah membujuk seseorang melalui berbagai cara sebagaimana disebutkan dalam ketentuan tersebut, agar korban menyerahkan barang, membuat utang, atau menghapus piutang. Tindak pidana ini baru dianggap selesai (*voltooid*) apabila perbuatan pihak yang dirugikan telah terlaksana sebagaimana dikehendaki pelaku, dan penyerahan barang tidak harus dilakukan secara langsung kepada pelaku, melainkan dapat pula dilakukan kepada pihak lain yang ditunjuk atau disuruh oleh pelaku untuk menerimanya. Penjelasan pasal ini juga menegaskan bahwa daya upaya yang dapat menjadikan perbuatan menipu sebagai tindak pidana disebutkan secara limitatif, yakni penggunaan nama atau kedudukan palsu, penyalahgunaan keadaan, tipu muslihat, dan rangkaian kata bohong, dengan syarat adanya hubungan kausal antara daya upaya tersebut dan kepercayaan korban sehingga korban bersedia menyerahkan apa yang diminta pelaku.

Ditinjau dari struktur normatifnya, rumusan Pasal 492 KUHP Nasional dapat diuraikan ke dalam dua kelompok unsur, yaitu unsur objektif dan unsur subjektif. Unsur objektif tercermin dari rangkaian daya upaya yang digunakan pelaku untuk membujuk atau menggerakkan korban. Pertama, penggunaan nama atau martabat palsu, yaitu ketika pelaku memakai identitas yang bukan miliknya sendiri, atau kedudukan yang tidak sesuai dengan keadaan sebenarnya, termasuk penambahan gelar atau status yang tidak faktual. Kedua, rangkaian kebohongan, yang tidak cukup diwujudkan dalam satu pernyataan bohong saja, melainkan serangkaian kebohongan yang tersusun sedemikian rupa hingga membentuk narasi yang tampak logis dan meyakinkan, di mana satu pernyataan memperkuat pernyataan lainnya. Ketiga, tipu muslihat, yakni perbuatan yang dilakukan dengan akal licik dan daya upaya menyesatkan sehingga korban menjadi percaya atas kebenaran suatu keadaan, termasuk melalui penunjukan dokumen atau bukti palsu. Keempat, unsur menggerakkan orang lain, yang dimaknai sebagai bentuk pengaruh yang dilakukan pelaku sedemikian rupa sehingga korban bertindak sesuai kehendak pelaku untuk menyerahkan barang. Kelima, objek berupa barang, baik yang berwujud seperti uang, pakaian, atau kendaraan, maupun yang tidak berwujud seperti aliran listrik atau gas. Keenam, akibat berupa timbulnya utang atau terhapusnya piutang, yang merupakan bentuk kerugian materiil bagi korban akibat tindakan yang digerakkan oleh pelaku. Adapun unsur subjektifnya terletak pada kesengajaan (*dolus*) untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, yang menurut Moeljatno mengandung dua corak, yaitu kesengajaan sebagai kepastian dan kesengajaan sebagai kemungkinan¹⁹.

Kerangka normatif klasik tersebut kini dihadapkan pada tantangan baru seiring munculnya teknologi *deepfake*, yaitu rekayasa audiovisual berbasis kecerdasan buatan yang mampu meniru wajah, suara, ekspresi, dan pola bicara seseorang secara hiperrealistis sehingga sulit dibedakan dari aslinya. Teknologi ini bekerja dengan memanfaatkan model pembelajaran mendalam yang memproses data dalam jumlah besar untuk menghasilkan manipulasi visual maupun audio yang tampak otentik meskipun sesungguhnya palsu. Ketika dikombinasikan dengan jangkauan penyebaran media sosial yang masif dan cepat, *deepfake* menjadi sarana baru bagi pelaku kejahatan

¹⁹Moeljatno, *Asas-Asas Hukum Pidana*, Rineka Cipta, Jakarta, 2008, hlm. 176–177.

untuk membangun kepercayaan palsu di hadapan korban dalam skala yang jauh lebih luas dibandingkan modus penipuan konvensional.

Perkembangan ini bukan sekadar ancaman teoretis, melainkan sudah tercermin dalam berbagai kasus nyata di Indonesia. seperti pada kasus penipuan berkedok bantuan sosial yang menggunakan wajah dan suara Presiden Prabowo Subianto²⁰. Dimana dalam menjalankan aksinya, pelaku mengambil video asli yang menampilkan Presiden Republik Indonesia Prabowo Subianto, Wakil Presiden Gibran Rakabuming Raka, dan Menteri Keuangan Sri Mulyani Indrawati. Video asli tersebut kemudian dimanipulasi menggunakan teknologi *Artificial Intelligence Deepfake* sehingga menghasilkan tampilan visual berupa gerakan bibir, ekspresi wajah, serta suara yang tampak alami dan seolah-olah para pejabat tersebut benar-benar sedang menyampaikan pengumuman resmi mengenai program bantuan pemerintah kepada masyarakat. Selanjutnya, video hasil manipulasi tersebut disebarluaskan melalui berbagai platform media sosial, khususnya Facebook, dengan mencantumkan nomor WhatsApp yang dapat dihubungi oleh masyarakat untuk memperoleh bantuan pemerintah yang dijanjikan. Melalui video tersebut, korban diarahkan untuk menghubungi nomor WhatsApp yang tertera, kemudian diminta mengisi formulir pendaftaran, menyerahkan data identitas berupa Kartu Tanda Penduduk (KTP), dan mengikuti proses verifikasi yang dibuat sedemikian rupa agar menyerupai prosedur resmi pemerintah. Setelah korban mempercayai proses tersebut, pelaku meminta korban melakukan transfer sejumlah uang dengan dalih sebagai biaya administrasi, biaya registrasi, ataupun biaya pencairan bantuan sosial. Bahkan, setelah korban melakukan pembayaran pertama, pelaku kembali meminta sejumlah uang tambahan dengan berbagai alasan administratif, padahal bantuan yang dijanjikan sama sekali tidak pernah ada.

Berdasarkan hasil penyidikan yang disampaikan oleh Dittipidsiber Bareskrim Polri, tersangka pertama yang berhasil diamankan adalah AMA (29 tahun), yang ditangkap pada 23 Januari 2025 di Lampung Tengah. Dalam proses pengembangan perkara, penyidik kemudian menetapkan seorang pelaku lain berinisial FA sebagai Daftar Pencarian Orang (DPO) karena diduga memiliki peran dalam proses pembuatan maupun pengeditan video *deepfake* yang digunakan dalam tindak pidana tersebut. Selanjutnya, pada 4 Februari 2025, penyidik kembali menangkap seorang tersangka lainnya berinisial JS (25 tahun) di Kabupaten Pringsewu, Provinsi Lampung, sebagai bagian dari pengembangan jaringan pelaku penipuan berbasis AI tersebut. Pada saat pengungkapan awal perkara tanggal 23 Januari 2025, penyidik mengidentifikasi sedikitnya 11 orang korban yang berasal dari berbagai daerah di Indonesia, antara lain Jawa Tengah, Jawa Timur, Sumatera Selatan, Sulawesi Tengah, serta beberapa daerah lainnya. Seiring berjalannya proses penyidikan dan bertambahnya laporan masyarakat, jumlah korban terus meningkat. Berdasarkan perkembangan penyidikan yang disampaikan oleh Dittipidsiber Bareskrim Polri pada 7 Februari 2025, jumlah korban telah mencapai 100 orang yang tersebar di 20 provinsi di Indonesia. Setiap korban diketahui mengalami kerugian dengan nominal yang bervariasi, yaitu berkisar antara Rp250.000,00 hingga Rp1.000.000,00 per orang. Secara keseluruhan, total kerugian yang berhasil didata oleh penyidik mencapai sekitar Rp65.000.000,00. Kementerian Komunikasi dan Digital mencatat bahwa potensi kerugian akibat penipuan berbasis

²⁰K. Meilina, 2025, "Penipuan Bansos Pakai AI Wajah Prabowo, Ratusan Korban Rugi," Katadata.co.id, 2025, sebagaimana dikutip dalam Y. S. Kristiyenda, J. Faradila, dan C. Basanova, "Pencegahan Kejahatan Deepfake: Studi Kasus terhadap Modus Penipuan Deepfake Prabowo Subianto dalam Tawaran Bantuan Uang," *Jurnal Politik, Sosial, Hukum dan Humaniora*, Vol. 3, No. 2.

deepfake diperkirakan mencapai sekitar Rp700 miliar²¹, sementara data Pusat Informasi Kriminal Nasional Bareskrim Polri mencatat puluhan ribu korban kejahatan siber sepanjang tahun 2025, meskipun penanganan yang secara khusus menyasar modus *deepfake* masih terbatas²².

Dari perspektif konstruksi hukum pidana, unsur-unsur dalam Pasal 492 KUHP Nasional pada dasarnya dapat direlevansikan dengan modus operandi penipuan berbasis *deepfake*. Penciptaan representasi digital seseorang yang menyerupai tokoh publik, pejabat, atau figur tepercaya lainnya dapat dikonstruksikan sebagai bentuk penggunaan “nama atau kedudukan palsu”, karena identitas yang ditampilkan kepada korban tidak sesuai dengan kenyataan. Manipulasi audio-visual yang dirancang agar tampak meyakinkan dapat dikategorikan sebagai “tipu muslihat”, sedangkan narasi manipulatif yang menyertai video atau audio *deepfake* – misalnya ajakan mentransfer dana atau menyerahkan barang atas nama pejabat tertentu – dapat memenuhi unsur “rangkaian kata bohong”. Ketika korban akhirnya menyerahkan uang, barang, atau membuat pengakuan utang akibat kepercayaannya terhadap konten *deepfake* tersebut, maka rangkaian unsur objektif dan subjektif dalam pasal penipuan pada dasarnya telah terpenuhi, sepanjang dapat dibuktikan adanya hubungan kausal antara tipu muslihat berbasis AI tersebut dan tindakan korban yang merugikan dirinya sendiri.

Selain KUHP Nasional, konstruksi hukum terhadap penipuan berbasis *deepfake* juga ditopang oleh sejumlah instrumen hukum lain yang saling melengkapi. Pasal 35 juncto Pasal 51 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik melarang “*setiap orang yang dengan sengaja dan tanpa hak melakukan manipulasi, penciptaan, perubahan, atau pengrusakan informasi maupun dokumen elektronik dengan tujuan agar dianggap seolah-olah otentik, dengan ancaman pidana penjara hingga dua belas tahun dan/atau denda hingga Rp12 miliar*” ketentuan yang secara konseptual relevan diterapkan pada penciptaan identitas digital palsu melalui *deepfake*. Di samping itu, penggunaan data biometrik seseorang berupa wajah atau suara tanpa persetujuan untuk membentuk konten *deepfake* juga berpotensi melanggar Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang mengatur sanksi administratif hingga pidana bagi pelanggarnya.

Kendati demikian, penegakan hukum terhadap penipuan berbasis *deepfake* masih menghadapi kesenjangan yang cukup signifikan, terutama pada aspek pembuktian. Undang-Undang Nomor 20 Tahun 2025 tentang Hukum Acara Pidana yang berlaku sejak Januari 2026 memang mewajibkan setiap alat bukti untuk dapat dibuktikan otentikasinya dan menegaskan bahwa bukti yang tidak otentik tidak dapat digunakan dalam persidangan, namun ketentuan tersebut belum disertai dengan mekanisme teknis yang secara khusus mengatur cara menguji otentikasi bukti yang dihasilkan atau dimanipulasi menggunakan kecerdasan buatan. Kesenjangan serupa juga ditemukan pada UU ITE, yang mengakui keabsahan bukti elektronik sepanjang integritasnya terjaga, tetapi belum mengatur secara rinci mekanisme pembuktian integritas untuk konten yang dihasilkan AI. Analisis forensik digital dalam perkara semacam ini pada praktiknya membutuhkan pemeriksaan metadata, pola piksel, dan artefak audio-visual

²¹Kementerian Komunikasi dan Digital Republik Indonesia, “*Deepfake Jadi Modus Kejahatan Siber Baru, Wamen Nezar Tegaskan Pentingnya Mitigasi Risiko*,” Siaran Pers, 22 Oktober 2025, <https://www.komdigi.go.id/berita/siaran-pers/detail/deepfake-jadi-modus-kejahatan-siber-baru-wamen-nezar-tegaskan-pentingnya-mitigasi-risiko>, diakses pada hari Kamis tanggal 09 Juli 2026 pukul 19.00 Wib.

²²Pusat Informasi Kriminal Nasional (Pusiknas) Bareskrim Polri, 2026, data korban kejahatan siber tahun 2025, sebagaimana dikutip dalam I. Mulyana, Y. M. Royani, dan T. Ludiana, “Kekosongan Hukum Mengenai Tindak Pidana Penipuan Deepfake dalam UU ITE Nomor 1 Tahun 2024 Menurut Perspektif Hukum Pidana Islam, *Jurnal Penelitian Hukum*, Vol. 2, No. 1.

yang sangat bergantung pada ketersediaan tenaga ahli forensik digital, sementara jumlah dan sebaran tenaga ahli tersebut di Indonesia belum merata²³. Kombinasi antara belum adanya regulasi yang secara eksplisit mendefinisikan *deepfake* sebagai delik tersendiri dan keterbatasan kapasitas forensik digital pada akhirnya menjadikan penegakan hukum terhadap kejahatan ini sangat bergantung pada penerapan pasal-pasal umum secara analogis, sehingga konsistensi putusan antar-perkara berpotensi berbeda-beda tergantung pada penafsiran hakim maupun kualitas alat bukti yang diajukan penuntut umum.

Secara keseluruhan, dapat disimpulkan bahwa konstruksi tindak pidana penipuan berbasis teknologi *deepfake* melalui media sosial dalam hukum pidana Indonesia saat ini dibangun melalui interpretasi ekstensif atas unsur-unsur konvensional dalam Pasal 492 KUHP Nasional, yang diperkuat oleh ketentuan Pasal 35 UU ITE dan UU Pelindungan Data Pribadi.²⁴ Meskipun kerangka hukum tersebut secara normatif cukup memadai untuk menjerat pelaku, efektivitas penagakannya masih bergantung pada penguatan kapasitas forensik digital, harmonisasi standar pembuktian otentikasi bukti elektronik berbasis AI dalam Hukum Acara Pidana yang baru, serta kemungkinan perumusan delik khusus *deepfake* di masa mendatang agar tidak seluruhnya bertumpu pada penerapan analogis atas pasal-pasal yang pada dasarnya dirancang untuk modus penipuan konvensional.

2. Pertanggungjawaban Pidana Terhadap Pelaku Penipuan Menggunakan Teknologi Deepfake Melalui Media Sosial

Perkembangan teknologi kecerdasan buatan (*artificial intelligence*), khususnya teknologi *deepfake*, telah melahirkan bentuk-bentuk baru tindak pidana penipuan yang beroperasi melalui manipulasi identitas visual dan suara seseorang dalam ruang digital. Dalam konteks hukum pidana Indonesia, persoalan ini menuntut analisis pertanggungjawaban pidana yang komprehensif, karena modus penipuan yang digunakan tidak lagi sekadar berbentuk rangkaian kata bohong atau tipu muslihat konvensional, tetapi berupa rekayasa informasi elektronik yang seolah-olah mencerminkan kehendak dan tindakan korban atas tindak pidana penipuan berbasis teknologi *deepfake* melalui media sosial sebagai objek kajian, sehingga pembahasan pertanggungjawaban pidana terhadap pelakunya harus dikonstruksi dengan merujuk pada kerangka normatif KUHP Nasional, UU ITE, serta teori-teori pertanggungjawaban pidana dan cybercrime yang telah dikemukakan dalam Bab I dan Bab II.

Rekayasa informasi elektronik yang menggunakan wajah dari seorang tokoh publik merupakan tindakan yang pastinya dilakukan dengan kesengajaan dikarenakan rangkaian tindakannya yang cukup panjang. Sengaja memiliki arti dimana seseorang dalam melakukan tindakannya membayangkan akan timbulnya akibat perbuatannya. Seseorang tidak dapat mengkehendaki akibat melainkan hanya dapat membayangkannya. Teori ini menitikberatkan pada apa yang diketahui atau dibayangkan oleh pelaku adalah apa yang terjadi pada waktu pelaku berbuat.²⁵ Dengan demikian, analisis yuridis yang disusun pada bagian ini bertujuan untuk menunjukkan bahwa pelaku penipuan dengan menggunakan teknologi *deepfake* tetap dapat dimintai pertanggungjawaban pidana meskipun modus operandi yang digunakan bersifat digital dan memanfaatkan celah regulasi yang belum sepenuhnya terakomodasi secara eksplisit dalam peraturan perundang-undangan positif.

Melihat perspektif KUHP Nasional, Melihat penjelasan Pasal 36 ayat (1) merupakan penegasan prinsip bahwa tiada pidana tanpa kesalahan, yang mana secara doktriner bentuk dari

²³ AHL Law Office, “*Penipuan Deepfake dan Jerat Hukum Pidana di Indonesia: Panduan Lengkap 2026*,” <https://ahl-lawoffice.com/artikel/hukum-pidana/penipuan-deepfake-dan-jerat-hukum-pidana-di-indonesia-panduan-lengkap-2026>, diakses pada hari Kamis tanggal 09 Juli 2026 pukul 20.00 Wib.

²⁴ SIP Law Firm, “*Pidana atas Konten Deepfake, Tantangan Baru Penegakan Hukum di Era AI*,” <https://siplawfirm.id/konten-deepfake>, diakses pada hari Kamis tanggal 09 Juli 2026 pukul 20.30 Wib.

²⁵ Sudarto, *Op Cit*, hlm.102

kesalahan dapat berupa kesengajaan dan kealpaan dan melihat rumusan tindak pidana penipuan dalam Pasal 492 Undang-Undang Nomor 1 Tahun 2023 memberikan dasar normatif yang cukup kuat untuk menginkorporasi penipuan berbasis teknologi *deepfake* sebagai bagian dari delik penipuan terhadap harta benda. Pasal tersebut menegaskan bahwa 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, dapat dipidana dengan pidana penjara dan/atau denda. Dengan memperhatikan perumusan unsur-unsur objektif dan subjektif dalam Bab II, tampak bahwa teknologi *deepfake* secara fungsional memenuhi kualifikasi sebagai sarana nama palsu, kedudukan palsu, maupun tipu muslihat dan rangkaian kebohongan dalam bentuk digital.

Dalam kasus-kasus konkret yang diuraikan dalam Bab I, seperti penggunaan wajah Gubernur Jawa Timur maupun Presiden untuk mengelabui korban melalui video *deepfake* di media sosial, pelaku secara sadar memanfaatkan identitas orang lain yang memiliki otoritas sosial dan politik untuk menumbuhkan kepercayaan korban sehingga mereka bersedia menyerahkan sejumlah uang. Pemakaian identitas digital korban atau tokoh publik di sini bukan sekadar penyalahgunaan nama, tetapi merupakan bentuk kedudukan palsu yang diperkuat melalui rekayasa visual dan audio. Oleh karena itu, unsur objektif berupa penggunaan nama atau kedudukan palsu sebagaimana dimaksud dalam Pasal 492 KUHP dapat dikatakan terpenuhi karena pelaku membangun representasi palsu mengenai siapa dirinya di hadapan korban, baik melalui profil akun maupun konten video yang didistribusikan.

Selanjutnya unsur tipu muslihat dan rangkaian kebohongan dalam Pasal 492 KUHP Nasional juga tampak jelas dalam modus penipuan berbasis *deepfake*. Tipu muslihat dipahami sebagai serangkaian tindakan dengan akal licik dan tipu daya untuk memperlakuk orang lain sehingga mereka tergerak memberikan sesuatu sesuai kehendak pelaku. Rangkaian kebohongan, pada gilirannya, bukan hanya satu perkataan bohong, melainkan beberapa kebohongan yang terstruktur sehingga membentuk narasi yang tampak logis dan dapat dipercaya. Dalam konteks penipuan *deepfake*, narasi yang dibangun pelaku tidak hanya berupa kata-kata dalam pesan teks atau caption, tetapi juga berupa audio-visual yang mempresentasikan tokoh tertentu sedang berbicara langsung kepada korban, misalnya menawarkan bantuan sosial, investasi, atau donasi tertentu.

Video *deepfake* yang meniru ekspresi wajah, gerak bibir, dan intonasi suara tokoh publik, ketika dikombinasikan dengan pesan-pesan elektronik melalui media sosial, menciptakan satu rangkaian kebohongan yang kompleks: korban tidak hanya dibohongi melalui kata-kata, tetapi juga melalui representasi visual yang seolah-olah autentik. Kecerdasan buatan mendapatkan data pribadi secara mudah melalui data-data pada media sosial yang mengumpulkan berbagai data dari para pengguna. Data ini kemudian dimanfaatkan untuk menciptakan konten manipulatif tanpa se pengetahuan individu yang bersangkutan, dan dapat menimbulkan risiko privasi yang serius.²⁶

Dengan demikian, unsur rangkaian kebohongan dan tipu muslihat dalam Pasal 492 KUHP tidak lagi terbatas pada komunikasi verbal tradisional, tetapi dapat diperluas pemaknaannya untuk mencakup rekayasa konten digital yang secara substansial memiliki efek yang sama, yakni menumbuhkan kepercayaan korban dan mendorong mereka melakukan tindakan yang merugikan diri sendiri. Konstruksi ini sejalan dengan perkembangan doktrin hukum pidana yang mulai mengakui bahwa manipulasi data dan sistem elektronik merupakan bentuk baru dari tipu muslihat dan rangkaian kebohongan dalam konteks penipuan online sesuai dengan apa yang dimuat dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Melihat perspektif unsur subjektif, penipuan berbasis teknologi *deepfake* melalui media sosial jelas memenuhi elemen kesengajaan (*dolus*) sebagaimana dijelaskan oleh Moeljatno dan para pakar lain dalam Bab II. Pelaku secara sadar merencanakan penggunaan teknologi *deepfake*, memilih wajah atau identitas digital korban atau tokoh publik, menyusun skenario narasi

²⁶ Hazmin Sulton Firdaus dan Lona Puuspita, 2025, "Peran Hukum Dalam Mengatasi Penyebaran Konten Deepfake Untuk Penipuan Identitas Digital", *UIR LawReview*, Vol 9, No.1

penipuan, dan mendistribusikan konten tersebut melalui platform media sosial yang memiliki jangkauan luas. Tidak ada ruang bagi penafsiran bahwa tindakan tersebut dilakukan karena kelalaian semata (*culpa*), sebab proses pembuatan dan penyebaran video *deepfake* menuntut serangkaian langkah teknis dan keputusan yang hanya dapat terjadi apabila pelaku memiliki kehendak dan pengetahuan yang cukup mengenai konsekuensi dari perbuatannya.

Lebih jauh lagi, maksud menguntungkan diri sendiri atau orang lain secara melawan hukum tampak nyata dalam kasus yang dijelaskan pada BAB III, dimana pelaku berhasil meraup keuntungan puluhan juta rupiah dari sejumlah korban yang tersebar di berbagai daerah. Perbuatan tersebut bukan saja merugikan korban secara materiil, tetapi juga merusak kepercayaan masyarakat terhadap figur-figur publik yang wajahnya disalahgunakan. Dalam kerangka teori pertanggungjawaban pidana Hans Kelsen yang digunakan sebagai landasan teoritis dalam Bab I, pelaku penipuan *deepfake* menanggung pertanggungjawaban individual atas pelanggaran yang dilakukan dengan sengaja, karena ia merupakan subjek utama dari perilaku yang ditetapkan oleh tatanan hukum sebagai syarat pemberian sanksi.

Dalam kaitannya dengan UU ITE sebagai *lex specialis* di bidang informasi dan transaksi elektronik, penipuan berbasis teknologi *deepfake* melalui media sosial merupakan bentuk manipulasi informasi elektronik yang diatur dalam Pasal 35 UU ITE dan sanksinya dalam Pasal 51 ayat (1). Pasal 35 menegaskan bahwa setiap orang yang dengan sengaja dan tanpa hak melakukan manipulasi, penciptaan, perubahan, penghilangan, atau perusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi tersebut dianggap seolah-olah data yang otentik, dapat dipidana. Video atau gambar *deepfake* pada hakikatnya adalah hasil penciptaan dan manipulasi informasi elektronik yang menampilkan seolah-olah tokoh tertentu melakukan pernyataan atau tindakan tertentu, padahal konten tersebut tidak pernah terjadi dalam kenyataan. Selain itu, Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP) memberikan kerangka hukum terkait pengelolaan data pribadi. Pada Pasal 65 UU PDP menegaskan bahwa dalam penggunaan data pribadi haruslah dilakukan dengan persetujuan eksplisit dari pemilik data.²⁷ Turan tersebut, meskipun memberikan perlindungan terhadap data biometrik seperti wajah, suara, atau sidik jari, tetap memiliki kekurangan dalam menangani penyalahgunaan data pribadi untuk pembuatan konten Deepfake. Hal ini dikarenakan UU PDP tidak secara eksplisit mencantumkan mekanisme penanganan pelanggaran berbasis teknologi AI, seperti Deepfake, yang memanfaatkan data biometrik untuk tujuan manipulasi. Deepfake pornografi menggambarkan kekhawatiran terkait pemalsuan video yang memanfaatkan kecerdasan buatan untuk menciptakan konten palsu yang sangat sulit dibedakan dari yang asli.²⁸

Selanjutnya konten *deepfake* tersebut digunakan sebagai sarana untuk menjerat korban dalam transaksi palsu, misalnya melalui permintaan transfer dana atau pengiriman bantuan, maka unsur penipuan sebagaimana diatur dalam Pasal 492 KUHP berkelindan dengan unsur manipulasi informasi elektronik dalam Pasal 35 UU ITE. Kombinasi ini memberi dasar bagi penegak hukum untuk menggunakan dakwaan kumulatif atau alternatif antara KUHP dan UU ITE, sebagaimana juga dikembangkan dalam praktik penegakan hukum terhadap kejahatan carding dan penipuan online lain yang memanfaatkan teknologi digital. Dengan demikian, pertanggungjawaban pidana terhadap pelaku penipuan *deepfake* tidak hanya bertumpu pada delik konvensional, tetapi juga memanfaatkan ketentuan khusus dalam UU ITE yang secara eksplisit mengatur konstruksi manipulasi data elektronik.

Perspektif teori cybercrime yang dikemukakan oleh Afrizal Zein dan Christien Rozali menilai bahwa penipuan berbasis teknologi *deepfake* dapat diklasifikasikan sebagai bentuk kejahatan siber yang memanfaatkan celah antara perkembangan teknologi dengan lambannya pembaruan regulasi. Dalam kerangka tersebut, teknologi bukan lagi sekadar sarana, melainkan menjadi bagian dari struktur kejahatan itu sendiri, karena tanpa adanya kemampuan untuk memproduksi *deepfake*, penipuan dengan modus tertentu tidak mungkin dilakukan. Oleh karena itu, pertanggungjawaban pidana terhadap pelaku penipuan *deepfake* harus mempertimbangkan

²⁷ *Ibid.*

²⁸ Rizki Kurniawan, Dkk., 2024, "Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi dan Pencurian Data Pribadi". *Jurnal Ilmiah Wahana Pendidikan*, Vol. 10 No. 10.

bahwa pelaku bukan hanya pengguna pasif teknologi, tetapi aktor yang secara aktif mengeksploitasi kemampuan teknologi untuk melakukan manipulasi identitas dan fakta.

Teori cybercrime juga menegaskan pentingnya pendekatan kebijakan kriminal yang integratif antara upaya penal (represif) dan non-penal (preventif), khususnya dalam menghadapi kejahatan yang lintas batas dan tidak mengenal teritorial seperti penipuan online. Dalam konteks penelitian ini, pertanggungjawaban pidana pelaku penipuan *deepfake* melalui media sosial tidak cukup hanya dilihat dari sisi pemidanaan, tetapi juga harus dikaitkan dengan kebutuhan akan regulasi khusus mengenai keamanan siber dan perlindungan data pribadi yang dapat mencegah penyalahgunaan teknologi *deepfake* secara masif. Dengan kata lain, kehadiran pelaku penipuan *deepfake* menjadi argumen empiris bagi urgensi pembaharuan hukum pidana.

Teori perlindungan hukum yang dikemukakan oleh Muhamad Sadi Is dalam Bab I juga relevan untuk memperkuat argumentasi pertanggungjawaban pidana terhadap pelaku penipuan *deepfake*. Dalam perspektif perlindungan hukum, negara berkewajiban memberikan perlindungan kepada warga negara dari segala bentuk penyalahgunaan teknologi yang dapat merugikan hak-hak mereka, baik hak ekonomi, hak atas privasi, maupun hak atas kehormatan dan reputasi. Penipuan berbasis *deepfake* melalui media sosial merupakan bentuk pelanggaran yang menggabungkan kerugian materiil dan immateriil sekaligus, karena korban tidak hanya kehilangan harta benda, tetapi juga mengalami kerusakan psikologis dan penurunan rasa aman dalam ruang digital.

Dengan demikian, pemidanaan terhadap pelaku penipuan *deepfake* tidak semata-mata berfungsi sebagai retribusi atas kesalahan yang dilakukan, tetapi juga sebagai instrumen perlindungan hukum bagi masyarakat luas. Putusan yang tegas dan proporsional terhadap pelaku penipuan *deepfake* akan memberikan efek jera dan sekaligus memberikan sinyal normatif bahwa negara tidak mentolerir penyalahgunaan teknologi kecerdasan buatan untuk tujuan kriminal. Di sisi lain, apabila penegak hukum ragu-ragu atau lamban dalam menerapkan ketentuan KUHP dan UU ITE terhadap kasus-kasus penipuan *deepfake*, maka negara dapat dianggap lalai dalam memenuhi kewajiban perlindungan hukum terhadap warganya.

Dalam perspektif sistem peradilan pidana, pertanggungjawaban pidana pelaku penipuan *deepfake* melalui media sosial juga harus dianalisis pada tahap pembuktian di pengadilan. Tantangan utama dalam perkara semacam ini adalah bagaimana hakim dapat meyakini bahwa konten *deepfake* memang dibuat dan didistribusikan oleh terdakwa, serta bagaimana membuktikan hubungan kausal antara konten tersebut dengan kerugian yang dialami korban. Dalam hal ini, pembuktian digital forensik menjadi sangat penting, karena hanya melalui analisis teknis terhadap metadata video, jejak digital di platform media sosial, dan hubungan antara akun pelaku dengan perangkat yang digunakan, aparat penegak hukum dapat membangun konstruksi perbuatan dan menautkannya dengan identitas terdakwa. Namun, tantangan pembuktian tidak boleh dijadikan alasan untuk mengabaikan pertanggungjawaban pidana pelaku penipuan *deepfake*. Justru, perkembangan kemampuan aparat penegak hukum dan ahli forensik digital harus dipandang sebagai bagian dari adaptasi sistem peradilan pidana terhadap kejahatan siber. Dalam kerangka teori pertanggungjawaban Kelsen, individu yang dikenai sanksi pidana atas dasar kejahatan *deepfake* harus merupakan subjek yang secara faktual dapat dibuktikan melakukan pelanggaran, dan sistem hukum harus menyediakan prosedur yang memadai untuk memastikan bahwa sanksi yang dijatuhkan benar-benar tertuju pada pelaku yang sebenarnya.

Dalam kaitannya dengan perkembangan kebijakan kriminalisasi penipuan online pasca berlakunya KUHP Baru dan UU ITE, terdapat kecenderungan bahwa Pasal 492 KUHP diposisikan sebagai norma umum yang fleksibel untuk mengakomodasi berbagai modus penipuan modern, termasuk yang berbasis teknologi *deepfake*. Hal ini tampak dari kajian-kajian doktrin yang menafsirkan unsur rangkaian kebohongan dan tipu muslihat sebagai mencakup manipulasi data dan sistem elektronik. UU ITE, sebagai *lex specialis*, memberikan penguatan terhadap konstruksi tersebut dengan menambahkan unsur manipulasi informasi elektronik sebagai perbuatan yang dilarang, sehingga penipuan *deepfake* dapat dipandang sebagai perbuatan yang berada di irisan antara hukum pidana materiil umum dan hukum pidana khusus di bidang elektronik.

Oleh karena itu, dalam merumuskan pertanggungjawaban pidana terhadap pelaku penipuan *deepfake*, jaksa penuntut umum idealnya menyusun dakwaan secara kumulatif atau alternatif antara Pasal 492 KUHP dan Pasal 35 jo. Pasal 51 ayat (1) UU ITE, sehingga hakim

memiliki ruang untuk mempertimbangkan pasal mana yang paling tepat diterapkan berdasarkan fakta persidangan. Pendekatan ini sejalan dengan asas legalitas dan asas *lex specialis derogat legi generali*, karena UU ITE tidak menghapus keberlakuan ketentuan KUHP, melainkan menambah lapisan pengaturan khusus untuk perbuatan yang berkaitan dengan teknologi informasi dan transaksi elektronik. Melihat perspektif keadilan substantif, pemidanaan terhadap pelaku penipuan *deepfake* melalui media sosial juga harus memperhatikan kepentingan korban dan masyarakat luas. Dalam banyak kasus, korban penipuan online adalah kelompok masyarakat yang memiliki literasi digital dan literasi finansial terbatas, sehingga mereka lebih mudah percaya kepada konten-konten yang tampak meyakinkan di media sosial. Penggunaan wajah tokoh publik atau pejabat negara melalui teknologi *deepfake* menambah derajat penyesatan terhadap korban, karena mereka percaya bahwa instruksi yang diterima berasal dari sumber yang legitimate. Dalam kerangka ini, pertanggungjawaban pidana pelaku penipuan *deepfake* tidak hanya terletak pada tindakan manipulasi data dan perolehan keuntungan secara melawan hukum, tetapi juga pada pelanggaran atas kepercayaan publik terhadap figur-figur tertentu dan terhadap sistem informasi digital itu sendiri. Oleh karena itu, hukuman yang dijatuhkan kepada pelaku harus mencerminkan derajat kesalahan dan dampak sosial dari perbuatannya. Pemidanaan yang terlalu ringan akan menimbulkan kesan bahwa negara tidak serius dalam menghadapi kejahatan siber, sedangkan pemidanaan yang terlalu berat tanpa pertimbangan proporsionalitas dapat menimbulkan persoalan baru terkait keadilan prosedural.

Penting pula untuk menyoroti dimensi pertanggungjawaban pidana korporasi dalam konteks penipuan *deepfake*, terutama apabila teknologi dan platform yang digunakan berada di bawah kendali badan hukum tertentu. Meskipun dalam kasus-kasus yang diteliti dalam tesis ini pelaku utama adalah individu yang memanfaatkan aplikasi *deepfake* yang tersedia secara umum, tidak menutup kemungkinan bahwa di masa depan akan muncul modus penipuan yang melibatkan perusahaan atau entitas digital yang secara sistematis memproduksi konten *deepfake* untuk tujuan penipuan massal. KUHP Baru dan UU ITE telah mulai mengakui korporasi sebagai subjek hukum pidana, sehingga pertanggungjawaban pidana dapat diperluas tidak hanya kepada individu pelaku, tetapi juga kepada badan hukum yang memperoleh keuntungan dari aktivitas penipuan tersebut atau lalai dalam mencegah penyalahgunaan sistemnya. Dalam perspektif kebijakan hukum pidana, pengaturan yang lebih tegas mengenai kewajiban platform digital untuk mendeteksi dan menghapus konten *deepfake* yang berpotensi menimbulkan penipuan merupakan bagian dari upaya preventif yang melengkapi pertanggungjawaban pidana individu. Namun, selama belum terdapat regulasi khusus yang secara eksplisit mengatur hal tersebut, fokus utama pertanggungjawaban pidana masih bertumpu pada individu pelaku yang secara langsung memproduksi dan menyebarkan konten *deepfake* untuk tujuan penipuan.

Dalam perkembangan terakhir, sejumlah kajian akademik menegaskan bahwa Pasal 492 UU No. 1 Tahun 2023 memang dirancang lebih responsif terhadap modus penipuan berbasis teknologi dibandingkan Pasal 378 KUHP lama, karena secara eksplisit mengakomodasi unsur penggunaan nama palsu, kedudukan palsu, tipu muslihat, dan rangkaian kebohongan dalam konteks kejahatan modern, termasuk penipuan online.²⁹ Hal ini mengatakan bahwa Pasal 492 KUHP baru memiliki substansi yang lebih komprehensif dan adaptif terhadap penipuan berbasis teknologi, sekaligus memberikan ruang bagi hakim untuk menilai tingkat kesalahan dan dampak kerugian secara lebih proporsional dalam menjatuhkan pidana. Sejalan dengan itu, kajian mengenai penipuan jual beli online dan penipuan dengan motif pemalsuan instrumen elektronik seperti QRIS juga mengonfirmasi bahwa penegak hukum cenderung menggunakan kombinasi Pasal 492 KUHP dan Pasal 35 UU ITE sebagai dasar dakwaan, sehingga pola ini secara teoritis dapat diterapkan pula terhadap penipuan menggunakan teknologi *deepfake* yang berbasis manipulasi data elektronik.³⁰

²⁹ S. Efendi, H. Sukarman, I. Setiawan, dan M. Amin Effendy, 2025, Analisis Tindak Pidana Penipuan Pasal 378 Undang-Undang Nomor 1 Tahun 1946 Dibandingkan dengan Pasal 492 Undang-Undang Nomor 1 Tahun 2023', *Pustaka Galuh Justisi*, Vol. 3, No. 2.

³⁰ Indra Mulyana dkk. 2026, Kekosongan Hukum mengenai Tindak Pidana Penipuan Deepfake dalam UU ITE Nomor 1 Tahun 2024', *Jurnal Ilmiah Galuh Justisi*, Vol. 14, No. 1.

Dalam konteks khusus *deepfake*, terdapat hal yang patut menjadi sorotan yaitu adanya kekosongan norma dalam Pasal 28 ayat (1) jo. Pasal 45A UU ITE, karena ketentuan tersebut masih berfokus pada berita bohong dan kerugian konsumen, sementara *deepfake* lebih tepat dipahami sebagai fabrikasi realitas sintetik yang menyesatkan persepsi korban tanpa selalu berkaitan dengan transaksi elektronik konsumen. Oleh karena itu, secara kebijakan, perlu adanya reformulasi kebijakan pidana diarahkan pada kriminalisasi eksplisit terhadap penyalahgunaan *deepfake* untuk tujuan penipuan dan pencemaran nama baik, serta perluasan pertanggungjawaban pidana terhadap pelaku dan korporasi yang memfasilitasi produksi maupun distribusi konten *deepfake* secara sistematis.

D. KESIMPULAN

1. Bahwa terhadap hukum positif di Indonesia dalam menghadapi tindak pidana penipuan berbasis teknologi *Deepfake* melalui media sosial secara keseluruhan konstruksi tindak pidana penipuan berbasis teknologi *deepfake* melalui media sosial dalam hukum pidana Indonesia saat ini dibangun melalui interpretasi ekstensif atas unsur-unsur konvensional dalam Pasal 492 KUHP Nasional, yang diperkuat oleh ketentuan Pasal 35 UU ITE dan UU PDP. Meskipun kerangka hukum tersebut secara normatif cukup memadai untuk menjerat pelaku, efektivitas penegakannya masih bergantung pada penguatan kapasitas forensik digital, harmonisasi standar pembuktian otentikasi bukti elektronik berbasis AI dalam Hukum Acara Pidana yang baru.
2. Bahwa melihat perspektif unsur subjektif pertanggungjawaban pidana, penipuan berbasis teknologi *deepfake* melalui media sosial jelas memenuhi elemen kesengajaan (*dolus*) dimana Pelaku secara sadar merencanakan penggunaan teknologi *deepfake*, memilih wajah atau identitas digital korban atau tokoh publik, menyusun skenario narasi penipuan, dan mendistribusikan konten tersebut melalui platform media sosial yang memiliki jangkauan luas. Tidak ada ruang bagi penafsiran bahwa tindakan tersebut dilakukan karena kelalaian semata (*culpa*), sebab proses pembuatan dan penyebaran video *deepfake* menuntut serangkaian langkah teknis dan keputusan yang hanya dapat terjadi apabila pelaku memiliki kehendak dan pengetahuan yang cukup mengenai konsekuensi dari perbuatannya.

E. SARAN

1. Diperlukannya perumusan delik khusus *deepfake* di masa mendatang agar tidak seluruhnya bertumpu pada penerapan analogis atas pasal-pasal yang pada dasarnya dirancang untuk modus penipuan konvensional ;
2. Secara kebijakan, perlu adanya reformulasi kebijakan pidana diarahkan pada kriminalisasi eksplisit terhadap penyalahgunaan *deepfake* untuk tujuan penipuan dan pencemaran nama baik, serta perluasan pertanggungjawaban pidana terhadap pelaku dan korporasi yang memfasilitasi produksi maupun distribusi konten *deepfake* secara sistematis.

DAFTAR PUSTAKA

- AHL Law Office, "Penipuan Deepfake dan Jerat Hukum Pidana di Indonesia: Panduan Lengkap 2026," <https://ahl-lawoffice.com/artikel/hukum-pidana/penipuan-deepfake-dan-jerat-hukum-pidana-di-indonesia-panduan-lengkap-2026>
- Ari Ayu Astuti, 2024, "Literasi Kemanfaatan Teknologi Terhadap kejahatan Terorganisir Lintas Batas Negara di Era Disrupsi dengan AI (Artificial Intelligence)", *Indonesian Journal of Criminal Law and Criminology*, Volume 5, Nomor 3
- DetikNews.com, "Pelaku Penipuan Deepfake Khofifah Raup Untung Rp 87 Juta Selama 3 Bulan", 30 April 2025, https://news.detik.com/berita/d-7892246/pelakupenipuandeepfake-khofifah-raup-untung-rp-87-juta-selama3bulan?utm_source=chatgpt.com
- Dimas Kresna Prayoga dan Ibrahim Fikma Edrisy, 2025, " Urgensi Pengaturan Hukum Terhadap Deepfake Sebagai Alat Kejahatan Siber Dalam Perspektif KUHP dan UU ITE", *Journal Evidence Of Law*, Volume 4, Nomor 3.
- Faisal Tamimi, Siti Munawaroh, 2024, "Teknologi Sebagai Kegiatan Manusia Dalam Era Modern Kehidupan Masyarakat", *Jurnal Teknologi dan Sistem Informasi*, Volume 2, Nomor.3
- Hazmin Sulton Firdaus dan Lona Puspita, 2025 , "Peran Hukum dalam Mengatasi Penyebaran Konten Deepfake Untuk Penipuan Identitas Digital", *UIRLawReview*, Vol. 9, No. 1.
- Indra Mulyana dkk. 2026, Kekosongan Hukum mengenai Tindak Pidana Penipuan Deepfake dalam UU ITE Nomor 1 Tahun 2024', *Jurnal Ilmiah Galuh Justisi*, Vol. 14, No. 1.
- K. Meilina, 2025, "Penipuan Bansos Pakai AI Wajah Prabowo, Ratusan Korban Rugi," *Katadata.co.id*, 2025, sebagaimana dikutip dalam Y. S. Kristiyenda, J. Faradila, dan C. Basanova, "Pencegahan Kejahatan Deepfake: Studi Kasus terhadap Modus Penipuan Deepfake Prabowo Subianto dalam Tawaran Bantuan Uang," *Jurnal Politik, Sosial, Hukum dan Humaniora*, Vol. 3, No. 2.
- Kementerian Komunikasi dan Digital Republik Indonesia, "Deepfake Jadi Modus Kejahatan Siber Baru, Wamen Nezar Tegaskan Pentingnya Mitigasi Risiko," *Siaran Pers*, 22 Oktober 2025, <https://www.komdigi.go.id/berita/siaran-pers/detail/deepfake-jadi-modus-kejahatan-siber-baru-wamen-nezar-tegaskan-pentingnya-mitigasi-risiko>
- Kompas.com, "Video "Deepfake" Prabowo Sudah Menelan 11 Korban dalam 4 Bulan Terakhir", 23 Januari 2025, https://nasional.kompas.com/read/2025/01/23/16382331/video-deepfake-prabowo-sudah-menelan-11-korban-dalam-4-bulan-terakhir?utm_source=chatgpt.com
- Moeljatno, *Asas-Asas Hukum Pidana*, Rineka Cipta, Jakarta, 2008.
- Muhammad Ramdhan, *Metode Penelitian*, Cipta Media Nusantara, Surabaya, 2021.
- Nabilah Purba, dkk., 2021, "Revolusi Industri 4.0 : Peran Teknologi Dalam Eksistensi Penguasaan Bisnis dan Implementasinya", *Jurnal Perilaku dan Strategi Bisnis*, Volume 9, Nomor 2
- Nadella Anggreani, "Pandangan Masyarakat Indonesia tentang UUIITE", *JDIH Kabupaten Tanah Laut*, Rabu 7 Mei 2025, https://jdih.tanahlautkab.go.id/artikel_hukum/detail/pandangan-masyarakat-indonesia-tentang-uu-ite/pandangan-masyarakat-indonesia-tentang-uuite#:~:text=1.jenis%2C%20dan%20prosedur%20transaksi%20elektronik
- Noor Rahmad, 2019, "Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online", *J-HES Jurnal Hukum Ekonomi Syariah*, Volume 3, Nomor 2.
- Pusat Informasi Kriminal Nasional (Pusiknas) Bareskrim Polri, 2026, data korban kejahatan siber tahun 2025, sebagaimana dikutip dalam I. Mulyana, Y. M. Royani, dan T. Ludiana, "Kekosongan Hukum Mengenai Tindak Pidana Penipuan Deepfake dalam UU ITE Nomor 1 Tahun 2024 Menurut Perspektif Hukum Pidana Islam, *Jurnal Penelitian Hukum*, Vol. 2, No. 1.
- Rachman Ma'ruf. Dkk, 2023, "Pengaturan Hukum Tindak Pidana Penipuan Secara Online Dalam Perspektif Hukum Pidana di Indonesia", *Jurnal Hukum dan Sosial Politik*, Volume 1, Nomor 2.
- Rendi Septiawan dkk, 2024, "Pemanfaatan Artificial Intelligence dalam Hukum Acara Pidana : Tinjauan Yuridis dan Dampak Sosial", *PERKARA Jurnal Ilmu Hukum dan Politik*, Volume 2, Nomor 4.
- Rizki Kurniawan, M., Nabila, T., Khalidy, A., Juniarti Tan, V., Widiyani, H., Huku Universitas Maritim Raja Ali Haji Abstrak, I., & Kunci, K, 2024, *Tinjauan Kriminologi Terhadap*

- Penyalahgunaan Artificial Intelligence: Deepfake Pornografi dan Pencurian Data Pribadi. Jurnal Ilmiah Wahana Pendidikan, Vol. 10, No. 10.
- S. Efendi, H. Sukarman, I. Setiawan, dan M. Amin Effendy, 2025, Analisis Tindak Pidana Penipuan Pasal 378 Undang-Undang Nomor 1 Tahun 1946 Dibandingkan dengan Pasal 492 Undang-Undang Nomor 1 Tahun 2023', Pustaka Galuh Justisi, Vol. 3, No. 2.
- Silvia Mah Arani Iskandar Putri, dkk, 2024, "Kriminalisasi Penggunaan Deepfake Dalam Tindak Pidana Penipuan Dan Pencemaran Nama Baik : Tantangan Dan Solusi Hukum", Jurnal Hukum Lagalita, Volume 6, Nomor 2.
- SIP Law Firm, "Pidana atas Konten Deepfake, Tantangan Baru Penegakan Hukum di Era AI," <https://siplawfirm.id/konten-deepfake>
- Sudarto, Hukum Pidana I, Badan Penyediaan Bahan-bahan kuliah Fakultas Hukum Universitas Diponegoro, Semarang, 1987.
- Sumarna Dadang dan Ayyub Kadriah, 2023, "Penelitian Kualitatif Terhadap Hukum Empiris," Jurnal Penelitian Serambi Hukum Vol. 16, No. 02.
- Wahyu Dwi Saputra, Dkk, 2026, " Kajian Terhadap Pertanggungjawaban Pidana Pelaku Kejahatan Siber (Cybercrime) Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik" Journal of Law, Social Science, And Management Review, Volume 2, Nomor 3.