



Relevansi Kepentingan Hukum Pelapor dengan Dakwaan dalam Perkara Deepfake

Reza Sukma Dewi¹, Ahmad Basuki²

Program Sarjana Fakultas Hukum, Universitas Wijaya Kusuma Surabaya, Indonesia¹⁻²

Email Korespondensi: rezsukmadew22@gmail.com, amd.basoeiki@gmail.com

Article received: 01 Januari 2026, Review process: 12 Januari 2026

Article Accepted: 22 Februari 2026, Article published: 01 Maret 2026

ABSTRACT

Deepfake is a technology that manipulates audio and visual data to depict a person as if they were performing or conveying something that never actually occurred. Such misuse has become a serious issue in society when it is employed as a means of fraud, the dissemination of false information, and the exploitation of personal data by unlawfully using the identity of public figures who are trusted by the public. This phenomenon is reflected in the case examined in this study entitled "The Application of Article 28 Paragraph (1) Juncto Article 45 Paragraph (2) of the Law on Information and Electronic Transactions against Deepfake Content Creators Causing Losses to Others (Case Study: Decision Number 124/Pid.B/2025/PN Gns)". This research employs a normative research method conducted through a literature review, using a statutory approach, a conceptual approach, and a case study approach. The results of the study indicate that the defendant's actions in creating and distributing deepfake content fulfill the elements of disseminating false and misleading information that causes losses to consumers. However, the application of Article 35 juncto Article 51 paragraph (1) of the Law on Information and Electronic Transactions is considered inappropriate, as it primarily emphasizes the manipulation of the authenticity of electronic data rather than the losses suffered by others. Therefore, Article 28 paragraph (1) juncto Article 45 paragraph (2) of the Law on Information and Electronic Transactions is deemed more appropriate for addressing digital fraud cases based on deepfake technology.

Keywords: Legal Protection, Fraud, Personal Data, Deepfake.

ABSTRAK

Deepfake merupakan teknologi manipulasi data audio dan visual yang mampu menampilkan seseorang seolah-olah melakukan atau menyampaikan sesuatu yang sebenarnya tidak pernah terjadi. Penyalahgunaan ini menjadi suatu persoalan di masyarakat ketika digunakan untuk sarana penipuan, penyebaran informasi bohong, serta adanya eksploitasi data pribadi dengan mencatut identitas publik figure yang dipercaya masyarakat. Contohnya ada pada kasus di dalam penelitian ini yang berjudul "Penerapan Pasal 28 Ayat (1) Juncto Pasal 45 Ayat (2) Undang-Undang Informasi dan Transaksi Elektronik terhadap Pembuat Konten Deepfake yang Menimbulkan Kerugian Orang Lain (Studi Kasus: Putusan Nomor 124/Pid.B/2025/PN Gns)" yang bertujuan yang pertama, untuk mengetahui dan menganalisis fakta hukum. Yang kedua, ketepatan penerapan ketentuan pidana terhadap pembuat konten deepfake yang menimbulkan kerugian bagi masyarakat. Dalam penulisan penelitian ini menggunakan metode penelitian normatif yang dilakukan melalui studi kepustakaan, dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan studi kasus. Berdasarkan hasil penelitian bahwa perbuatan terdakwa berupa

pembuatan dan penyebaran konten deepfake telah memenuhi unsur penyebaran berita bohong yang mengakibatkan kerugian konsumen. Namun demikian, penerapan Pasal 35 juncto Pasal 51 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik dinilai kurang tepat karena lebih menitikberatkan pada aspek manipulasi keotentikan data elektronik, bukan pada kerugian pada orang lain. Oleh karena itu, Pasal 28 ayat (1) juncto Pasal 45 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik lebih tepat digunakan dalam perkara penipuan digital berbasis deepfake.

Kata Kunci: *Perlindungan Hukum, Penipuan, Data Pribadi, Deepfake.*

PENDAHULUAN

Perkembangan kecerdasan buatan (Artificial Intelligence/AI) merupakan salah satu dampak nyata dari Revolusi Industri 4.0 yang membawa perubahan besar dalam berbagai aspek kehidupan manusia. AI dirancang untuk meniru kemampuan kognitif manusia, seperti belajar, mengenali pola, memahami bahasa, dan mengambil keputusan berbasis data. Di Indonesia, perkembangan AI menunjukkan percepatan yang signifikan seiring dengan meningkatnya infrastruktur digital, penetrasi internet, pemanfaatan big data, serta dukungan investasi dari sektor publik dan swasta. Kemajuan komputasi, algoritma pembelajaran mesin, dan jaringan digital berkecepatan tinggi menjadi fondasi utama berkembangnya aplikasi AI di berbagai sektor strategis (Haida, 2024).

Di satu sisi, AI memberikan berbagai manfaat, seperti peningkatan efisiensi dan produktivitas, pengembangan layanan publik, personalisasi layanan, serta munculnya inovasi dan peluang bisnis baru. AI telah dimanfaatkan dalam bidang kesehatan untuk membantu diagnosis penyakit, dalam pendidikan sebagai media pembelajaran adaptif, serta dalam industri untuk otomatisasi proses produksi. Namun, di sisi lain, perkembangan AI juga membawa risiko serius, seperti pelanggaran privasi, bias algoritma, ketimpangan sosial akibat otomatisasi, serta penyalahgunaan teknologi untuk tindak kejahatan berbasis digital (Chazawi, 2023).

Salah satu bentuk penyalahgunaan AI yang menimbulkan perhatian serius adalah teknologi deepfake, yaitu manipulasi wajah atau suara seseorang menggunakan jaringan saraf sehingga menghasilkan konten yang tampak sangat realistis. Deepfake menjadi problematik ketika digunakan untuk tujuan penipuan, pencemaran nama baik, dan penyebaran informasi palsu yang menyesatkan masyarakat. Teknologi ini berpotensi merugikan korban secara materiil maupun immateriil serta mengganggu kepercayaan publik terhadap informasi digital (Haida, 2024).

Fenomena tersebut tercermin dalam perkara pidana deepfake yang mencatut wajah Presiden Prabowo Subianto sebagaimana diputus dalam Putusan Nomor 124/Pid.B/2025/PN Gns. Dalam kasus ini, pelaku memanfaatkan foto dan video resmi Presiden yang diolah menggunakan teknologi AI untuk menciptakan video palsu seolah-olah Presiden menawarkan bantuan sosial. Video tersebut disebarluaskan melalui media sosial dan aplikasi pesan instan untuk menipu masyarakat, sehingga menyebabkan sekitar 100 orang dari berbagai provinsi mengalami kerugian finansial hingga puluhan juta rupiah (Tim detikcom, 2026).

Permasalahan hukum kemudian muncul terkait penerapan pasal yang digunakan dalam dakwaan. Jaksa menjerat terdakwa dengan Pasal 35 jo Pasal 51 ayat (1) UU ITE serta Pasal 378 KUHP tentang penipuan. Namun, Pasal 35 UU ITE pada dasarnya lebih menitikberatkan pada pemalsuan atau manipulasi keotentikan informasi elektronik, bukan pada dampak kerugian konsumen akibat rangkaian penipuan yang sistematis. Dalam konteks ini, karakter perbuatan terdakwa lebih menunjukkan adanya eksploitasi ekonomi melalui penyebaran berita bohong berbasis AI, sehingga memunculkan pertanyaan mengenai ketepatan konstruksi dakwaan yang digunakan (Chazawi, 2023).

Penelitian terdahulu telah menyoroti pentingnya perlindungan hukum bagi korban deepfake, tetapi masih terbatas pada kajian normatif secara umum. Oleh karena itu, penelitian ini memiliki kebaruan dengan fokus pada analisis konkret terhadap fakta hukum dan pertimbangan yuridis dalam putusan pengadilan, khususnya untuk menilai apakah penerapan Pasal 35 jo Pasal 51 ayat (1) UU ITE telah tepat atau justru perlu dikaitkan dengan pasal lain yang lebih relevan dengan sifat penipuan berbasis media sosial. Tujuan penelitian ini adalah untuk mengkaji ketepatan dakwaan dan putusan hakim dalam perkara deepfake tersebut serta memberikan pemahaman akademik mengenai pertanggungjawaban pidana atas penyalahgunaan AI yang menimbulkan kerugian bagi masyarakat.

METODE

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan kepustakaan yang menempatkan hukum sebagai sistem norma, mencakup analisis terhadap asas-asas, peraturan perundang-undangan, serta doktrin hukum yang relevan (Repository USM, 2018). Sesuai dengan klasifikasi yang dikemukakan oleh Soerjono Soekanto, penelitian ini mengkaji bahan hukum dari sudut sifat dan tujuannya melalui prosedur sistematis guna memperoleh kebenaran objektif (Soekanto, 2003). Metode pendekatan yang diterapkan meliputi pendekatan perundang-undangan, pendekatan konseptual, dan studi kasus untuk membedah permasalahan secara komprehensif sesuai teori Peter Mahmud Marzuki (Marzuki, 2017). Bahan hukum primer dikumpulkan melalui studi dokumen terhadap regulasi seperti UU ITE dan KUHP, sementara bahan hukum sekunder digunakan untuk memperkuat argumentasi melalui literatur ilmiah dan opini hukum (Soekanto & Mamudji, 2015). Analisis dilakukan secara deskriptif-analitis terhadap kasus manipulasi konten *deepfake* untuk menentukan ketepatan penerapan pasal pidana dan memahami implikasi teknologi kecerdasan buatan dalam ruang digital (Populix, 2024).

HASIL DAN PEMBAHASAN

Fakta-Fakta Hukum

Dalam perkara Nomor 124/Pid.B/2025/PN Gns, terdakwa berinisial AMA terbukti menyebarkan konten deepfake wajah Presiden Prabowo Subianto untuk menipu masyarakat dengan iming-iming bantuan sosial fiktif (Kurniawan Fadilah, 2026). Modus operandi ini dilakukan dengan mengarahkan korban menghubungi nomor WhatsApp tertentu dan meminta transfer biaya administrasi yang

mengakibatkan kerugian materiil hingga puluhan juta rupiah (CNN Indonesia, 2025). Berdasarkan hasil analisis forensik digital, video tersebut dikonfirmasi sebagai rekayasa kecerdasan buatan yang menggunakan teknik deep learning Generative Adversarial Network atau GAN (Fernandes & Fatma, 2025). Kejahatan ini menunjukkan bahwa figur publik hanya dijadikan alat manipulasi, sementara korban utamanya adalah masyarakat luas yang tertipu oleh keaslian visual konten hasil rekayasa digital tersebut.

1) Kronologi Terjadinya Tindak Pidana Penyebaran Konten Deepfake

Kejahatan manipulasi informasi ini dilakukan secara terstruktur melalui lima tahap utama, mulai dari persiapan konten palsu menggunakan teknologi AI hingga proses penangkapan pelaku oleh pihak kepolisian. Terdakwa AMA memodifikasi data visual Presiden Prabowo Subianto dan pejabat negara lainnya menjadi video *deepfake* autentik yang memuat narasi bohong mengenai bantuan sosial tunai (Putusan Nomor 124/Pid.B/PN Gns, 2026). Setelah konten disebarluaskan di media sosial, terdakwa menjerat korban melalui skema penipuan biaya administrasi fiktif yang dilakukan secara sistematis lewat komunikasi WhatsApp. Rangkaian tindak pidana ini berakhir setelah Direktorat Tindak Pidana Siber Bareskrim Polri melakukan pelacakan jejak digital dan menangkap para pelaku di wilayah Lampung pada awal tahun 2025.

2) Fakta Kerugian Korban

Fakta kerugian dalam perkara Nomor 124/Pid.B/2025/PN Gns dibuktikan melalui keterangan saksi, bukti transfer dana, serta rekaman percakapan elektronik yang menunjukkan adanya penipuan sistematis. Para korban mentransfer uang dalam nominal bervariasi melalui bank maupun dompet digital setelah terperdaya oleh instruksi biaya administrasi fiktif yang tercantum dalam video *deepfake* tersebut (Putusan Nomor 124/Pid.B/2025/PN Gns, 2026). Hingga persidangan berlangsung, dana tersebut tidak pernah dikembalikan dan bantuan sosial yang dijanjikan terbukti tidak pernah ada. Akumulasi kerugian materiil dari puluhan korban di berbagai wilayah Indonesia dilaporkan mencapai puluhan juta rupiah, yang disertai pula dengan dampak psikologis berupa hilangnya kepercayaan publik terhadap informasi di media sosial.

3) Fakta Alat Bukti Elektronik

Dalam persidangan perkara Nomor 124/Pid.B/2025/PN Gns, Jaksa Penuntut Umum mengajukan berbagai informasi dan dokumen elektronik sebagai alat bukti hukum yang sah sesuai dengan ketentuan Undang-Undang ITE (Undang-Undang Nomor 11 Tahun 2008). Alat bukti utama berupa file video *deepfake* Presiden RI yang memiliki kualitas visual menyerupai rekaman resmi diperlihatkan di hadapan Majelis Hakim untuk membuktikan adanya rekayasa konten. Selain itu, tangkapan layar unggahan media sosial dan rekaman percakapan WhatsApp digunakan untuk menunjukkan penyebaran konten secara luas serta instruksi penipuan biaya administrasi kepada para korban (Ahmad Ramli, 2019). Bukti transaksi elektronik berupa aliran dana ke dompet digital terdakwa melengkapi rangkaian pembuktian mengenai kerugian materiil yang dialami masyarakat. Seluruh bukti tersebut telah

diverifikasi keasliannya melalui proses penyidikan guna menjamin validitas pembuktian dalam sistem peradilan pidana.

4) Fakta Keterangan Saksi

Dalam persidangan perkara Nomor 124/Pid.B/2025/PN Gns, Jaksa Penuntut Umum menghadirkan saksi korban dan saksi penyidik yang memberikan keterangan di bawah sumpah guna memperjelas rangkaian tindak pidana terdakwa. Saksi korban secara konsisten menerangkan bahwa kepercayaan mereka terhadap informasi bantuan sosial muncul karena video tersebut menampilkan sosok Presiden Republik Indonesia, yang kemudian berlanjut pada komunikasi WhatsApp dan instruksi transfer biaya administrasi. Di sisi lain, saksi dari pihak kepolisian memaparkan hasil penelusuran digital yang membuktikan bahwa akun media sosial serta nomor WhatsApp yang digunakan untuk menyebarkan konten *deepfake* terhubung langsung dengan perangkat milik terdakwa. Seluruh keterangan saksi tersebut saling bersesuaian dan sinkron dengan alat bukti elektronik lainnya dalam menggambarkan bagaimana manipulasi digital ini mengakibatkan kerugian nyata bagi masyarakat luas. Penjelasan para saksi memperkuat pembuktian bahwa terdakwa secara sadar menjalankan skema penipuan terorganisir dengan memanfaatkan figur otoritas negara sebagai alat pengelabuan (Putusan Nomor 124/Pid.B/PN Gns, 2026).

5) Fakta Keterangan Ahli

Dalam persidangan, Jaksa Penuntut Umum menghadirkan ahli teknologi informasi dan forensik digital yang mengonfirmasi bahwa video barang bukti merupakan hasil rekayasa kecerdasan buatan melalui teknik pembelajaran mesin. Ahli menjelaskan bahwa analisis forensik menemukan ketidaksesuaian pola gerak bibir serta struktur suara yang membuktikan adanya manipulasi digital untuk meniru figur pejabat negara secara realistis. Teknologi *deepfake* ini sengaja dirancang agar tampak seperti pernyataan resmi sehingga masyarakat awam sulit membedakan keasliannya dari rekaman orisinal (Arifin & Seftiniara, 2022). Karakteristik video tersebut memungkinkan distribusi informasi elektronik secara masif melalui media sosial, yang secara teknis berpotensi menimbulkan dampak kerugian luas dalam waktu singkat.

6) Fakta Keterangan Terdakwa

Terdakwa AMA dalam persidangan mengakui secara langsung bahwa ia membuat video *deepfake* Presiden menggunakan perangkat pribadinya dengan memanfaatkan materi visual dari internet. Ia membenarkan telah menyebarkan video tersebut ke media sosial dan mengelola sendiri nomor WhatsApp untuk menipu masyarakat melalui iming-iming bantuan sosial fiktif. Terdakwa juga mengakui telah menerima dan menggunakan dana transfer dari para korban untuk kepentingan pribadi meskipun mengetahui bahwa program bantuan tersebut tidak pernah ada. Pengakuan ini memperkuat kesesuaian antara alat bukti elektronik dan keterangan saksi yang secara utuh menggambarkan peran sentral terdakwa dalam seluruh rangkaian peristiwa pidana tersebut.

7) Unsur Actus Reus dan Mens Rea dalam Kasus Penyebaran Konten Deepfake

Pertanggungjawaban pidana terdakwa AMA dalam kasus deepfake ini terpenuhi melalui analisis dua unsur fundamental, yaitu actus reus dan mens rea (Deardorff, 2026). Unsur actus reus (perbuatan lahiriah) terbukti dari serangkaian tindakan konkret terdakwa yang meliputi pembuatan konten palsu berbasis AI, distribusi video hoaks melalui media sosial, hingga tindakan pengelabuan konsumen yang menyebabkan kerugian materiil nyata (Budiastanti, 2017). Sementara itu, unsur mens rea (niat jahat) tampak jelas melalui kesengajaan (*dolus directus*) terdakwa yang merencanakan penipuan demi motif keuntungan ekonomi pribadi (Kurniawan Fadilah, 2026). Perpaduan antara perbuatan melawan hukum yang selesai dilakukan dan adanya niat buruk untuk menipu publik menunjukkan bahwa terdakwa secara sadar bertanggung jawab penuh atas tindak pidana penyebaran informasi menyesatkan yang merugikan masyarakat tersebut.

8) Analisa Fakta Hukum Terhadap Penerapan Pasal 28 ayat (1) Jo Pasal 45 ayat (2) UU ITE

Berdasarkan fakta hukum yang terurai, terdakwa AMA terbukti secara sah melakukan manipulasi audio-visual menggunakan teknologi AI untuk menyebarkan berita bohong yang menyesatkan masyarakat. Tindakan pencatutan identitas Presiden Prabowo Subianto merupakan sarana untuk membangun kepercayaan publik, sementara kerugian materiil yang nyata justru dialami oleh masyarakat yang melakukan transfer dana bantuan fiktif. Seluruh unsur dalam Pasal 28 ayat (1) jo Pasal 45 ayat (2) UU ITE telah terpenuhi karena terdakwa merupakan subjek hukum yang cakap dan terbukti melakukan penipuan melalui transaksi elektronik. Dalam perspektif viktimologi, masyarakatlah yang berkedudukan sebagai korban langsung yang berhak mendapatkan perlindungan hukum, mengingat fokus delik ini adalah pada kerugian materiil konsumen di ruang digital.

Dakwaan

1) Dakwaan Primair

Jaksa Penuntut Umum mengajukan dakwaan primair berdasarkan Pasal 35 jo. Pasal 51 ayat (1) UU ITE yang fokus pada larangan memanipulasi informasi elektronik agar dianggap seolah data autentik (Chazawi & Ferdian, 2015). Terdakwa secara aktif dan sengaja menggunakan teknologi *deepfake* berbasis *Generative Adversarial Network* (GAN) untuk memalsukan identitas Presiden, sebuah tindakan yang melampaui distribusi konten pasif karena memerlukan keahlian teknis khusus (Fernandes & Fatma, 2025). Meskipun Majelis Hakim menyatakan dakwaan ini terbukti secara teknis, terdapat kritik akademik yang menilai bahwa Pasal 35 UU ITE terlalu menitikberatkan pada aspek keaslian data (*data authenticity*) dibandingkan dampak sosial-ekonomi nyata berupa kerugian materiil konsumen (Kaunang, 2024). Hal ini menunjukkan adanya keterbatasan konseptual dalam dakwaan primair tersebut karena belum mengeksplorasi hubungan kausal antara manipulasi digital dan perlindungan hak korban secara komprehensif (Ratnawati et al., 2023).

2) Dakwaan Subsidiar

Dakwaan subsidair dalam perkara Nomor 124/Pid.B/2025/PN Gns disusun sebagai jaring pengaman yuridis (*legal safety net*) dengan menjerat terdakwa menggunakan Pasal 378 KUHP tentang penipuan (Harahap, 2016). Jaksa Penuntut Umum menguraikan bahwa terdakwa secara sadar menggunakan identitas dan martabat palsu sebagai petugas pemerintah guna menggerakkan para korban mentransfer uang administrasi bantuan sosial fiktif (Hamzah, 2010). Unsur penipuan terpenuhi melalui rangkaian kebohongan sistematis, mulai dari penggunaan video *deepfake* hingga komunikasi persuasif via WhatsApp yang mengakibatkan kerugian materiil nyata pada puluhan korban (Budiastanti, 2017). Meskipun Pasal 378 KUHP dapat menjangkau perbuatan terdakwa, secara akademik pasal ini dianggap sebagai *lex generalis* yang belum spesifik mengatur karakteristik penipuan berbasis teknologi informasi dibandingkan dengan pasal-pasal dalam UU ITE (Ama & Kadir, 2024).

3) Analisa Dakwaan

Berdasarkan analisis terhadap dakwaan primair dan subsidair, penggunaan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE dinilai jauh lebih relevan untuk menjerat perbuatan terdakwa AMA karena kesesuaiannya dengan karakteristik tindak pidana yang dimulai dari penyebaran konten *deepfake* hingga timbulnya kerugian materiil. Terdakwa secara sadar menyebarkan berita bohong dan menyesatkan mengenai bantuan sosial fiktif yang mengakibatkan masyarakat, dalam kedudukannya sebagai konsumen informasi, melakukan transaksi elektronik berupa transfer dana melalui layanan perbankan dan dompet digital. Meskipun dakwaan Pasal 35 UU ITE dan Pasal 378 KUHP telah diajukan, Pasal 28 ayat (1) memberikan perlindungan hukum yang lebih spesifik dan kuat karena secara eksplisit mengatur hubungan kausal antara penyebaran berita bohong dengan kerugian nyata yang dialami masyarakat dalam transaksi elektronik. Dengan demikian, penerapan pasal ini memberikan kepastian hukum yang lebih tepat dalam merespons eskalasi kejahatan berbasis manipulasi kecerdasan buatan (Putusan Nomor 124/Pid.B/2025/PN Gns, 2026).

Analisis terhadap Dakwaan Penuntut Umum

Menurut Lilik Mulyadi, surat dakwaan merupakan jantung perkara pidana karena menjadi dasar pembatas pemeriksaan hakim, pembuktian jaksa, dan pembelaan terdakwa (Mulyadi, 2019). Oleh karena itu, ketepatan dakwaan tidak hanya bersifat formal, tetapi juga substantif agar tidak menimbulkan ketidakadilan. Dalam Perkara Nomor 124/Pid.B/2025/PN Gns, Penuntut Umum mendasarkan dakwaan pada Pasal 35 jo Pasal 51 ayat (1) UU ITE serta Pasal 378 KUHP. Sekilas, dakwaan tersebut tampak relevan karena terdakwa terbukti memanipulasi video *deepfake* dan menggunakannya untuk penipuan. Namun, analisis lebih lanjut menunjukkan dakwaan terlalu menitikberatkan aspek manipulasi data elektronik. Padahal, fakta persidangan memperlihatkan bahwa kerugian utama dialami masyarakat sebagai korban penipuan. Perbedaan antara fokus dakwaan dan realitas kerugian korban ini menimbulkan persoalan yuridis terkait ketepatan arah penuntutan (Hamzah, 2018).

Fakta persidangan menunjukkan bahwa manipulasi video deepfake hanyalah sarana untuk melakukan penipuan digital yang menimbulkan kerugian materiil bagi masyarakat. Dakwaan Penuntut Umum yang menjadikan Pasal 35 UU ITE sebagai pasal utama cenderung menempatkan pencatutan identitas sebagai fokus perlindungan hukum. Akibatnya, posisi korban yang sesungguhnya, yaitu masyarakat yang mengalami kerugian ekonomi, menjadi terpinggirkan. Padahal, dalam hukum pidana modern, orientasi perlindungan hukum seharusnya diarahkan pada dampak nyata perbuatan pidana. Pemisahan antara kejahatan manipulasi elektronik dan penipuan konvensional juga berpotensi mengaburkan karakter kejahatan siber yang utuh. Kesalahan konstruksi dakwaan dapat berdampak pada lemahnya perlindungan korban dan efektivitas pemidanaan. Oleh karena itu, pemilihan pasal yang tepat dan berorientasi pada perlindungan korban menjadi krusial dalam penegakan hukum kejahatan digital (Arief, 2018).

Analisis Putusan No. 124/Pid.B/2025/PN Gns

Putusan Nomor 124/Pid.B/2025/PN Gns menjadi tonggak penting dalam penegakan hukum siber di Indonesia karena secara eksplisit menangani kejahatan berbasis teknologi *deepfake*. Perkara ini melibatkan terdakwa AMA (Almandela) yang didakwa secara berlapis dengan dakwaan primair Pasal 35 jo. Pasal 51 ayat (1) UU ITE terkait manipulasi data otentik, serta dakwaan subsidair Pasal 378 KUHP tentang penipuan konvensional. Majelis Hakim Pengadilan Negeri Gunung Sugih dalam amar putusannya menyatakan terdakwa terbukti secara sah dan meyakinkan bersalah, yang mana proses hukum ini dipandang sebagai sarana penemuan hukum (*rechtsvinding*) untuk menghadapi kompleksitas *cybercrime* di masa depan (Mertokusumo dalam Putusan PN Gns, 2025).

Dalam pertimbangannya, Majelis Hakim menitikberatkan pada pemenuhan unsur subjektif berupa kesengajaan (*dolus*) dan unsur objektif berupa penciptaan informasi elektronik palsu yang menyerupai pernyataan resmi Presiden RI. Hakim menerapkan asas *lex specialis derogat legi generali* dengan memprioritaskan UU ITE sebagai aturan khusus, didukung oleh bukti digital berupa analisis forensik dan keterangan ahli yang mengonfirmasi penggunaan teknologi *Generative Adversarial Network* (GAN) (Fernandes & Fatma, 2025). Meskipun secara formal unsur manipulasi terpenuhi, terdapat catatan kritis bahwa fokus hakim lebih tertuju pada aspek teknis keotentikan data daripada dampak ekonomi yang diderita oleh masyarakat sebagai korban nyata (Marzuki, 2017).

Analisis akademik menunjukkan adanya keterbatasan konseptual pada penerapan Pasal 35 UU ITE dalam kasus ini, mengingat pasal tersebut lebih melindungi integritas sistem informasi daripada kerugian materiil pengguna. Identitas Presiden dalam perkara ini hanyalah objek pencatutan identitas untuk membangun kepercayaan, sedangkan korban sesungguhnya adalah masyarakat, seperti Musakkir dan Nur Ahmad Nawawi, yang mengalami kerugian finansial akibat penipuan tersebut (R. Soesilo dalam Putusan PN Gns, 2025). Oleh karena itu, muncul argumentasi bahwa Pasal 28 ayat (1) jo. Pasal 45 ayat (2) UU ITE seharusnya lebih relevan digunakan karena secara spesifik mengatur tentang berita bohong

yang mengakibatkan kerugian konsumen dalam transaksi elektronik, sehingga memberikan perlindungan hukum yang lebih substantif dan adil bagi para korban.

SIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa Pasal 28 ayat (1) jo Pasal 45 ayat (2) UU ITE berorientasi pada perlindungan masyarakat atau konsumen yang mengalami kerugian nyata akibat penyebaran berita bohong, sedangkan Pasal 35 jo Pasal 51 ayat (1) UU ITE lebih menitikberatkan pada perlindungan keotentikan informasi elektronik. Dalam Perkara Nomor 124/Pid.B/2025/PN Gns, penerapan Pasal 35 jo Pasal 51 ayat (1) UU ITE dan Pasal 378 KUHP secara normatif dapat dibenarkan karena adanya manipulasi video deepfake, namun secara substantif kurang tepat karena tidak sepenuhnya melindungi korban yang mengalami kerugian materiil, yaitu masyarakat, sementara pihak yang identitasnya dicatut tidak mengalami kerugian langsung. Oleh karena itu, disarankan agar penyidik dan penuntut umum lebih cermat dalam memilih konstruksi pasal dengan mempertimbangkan akibat perbuatan dan kedudukan korban, serta hakim diharapkan tidak hanya menilai pemenuhan unsur delik secara normatif, tetapi juga memperhatikan tujuan hukum pidana berupa keadilan, kemanfaatan, dan perlindungan korban.

UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada dosen pembimbing yang telah memberikan arahan dan bimbingan selama proses penelitian ini. Terima kasih juga disampaikan kepada pihak yang telah memberikan kontribusi dalam pelaksanaan penelitian ini. Terakhir, penulis menyampaikan apresiasi kepada Al-Zayn: Jurnal Ilmu Sosial & Hukum atas kesempatan untuk mempublikasikan hasil penelitian ini.

DAFTAR RUJUKAN

- Ama, Jefrianus Tamo & Kadir, Syukron Abdul. (2024). Tinjauan yuridis terhadap tindak pidana penipuan online. *Media Hukum Indonesia*, Vol. 2 No. 2.
- Arifin, Ridwan & Seftiniara, Intan Nurina. (2022). Tantangan penegakan hukum terhadap kejahatan deepfake. *Jurnal Ilmu Hukum*, Vol. 10 No. 2.
- Budiastanti, Dhaniar Eka. (2017). Perlindungan hukum terhadap korban penipuan melalui internet. *Jurnal Cakrawala Hukum*, Vol. 8 No. 1.
- Chazawi, Adami & Ferdian, Ardi. (2015). *Tindak Pidana Informasi dan Transaksi Elektronik*. Malang: Media Nusa Creative.
- CNN Indonesia. (2025). Modus penipuan deepfake AI Prabowo-Gibran: Tawarkan bantuan uang.
- Deardorff, Alex. (2026). *Actus reus vs. mens rea*.
- Fernandes, Yoggy Arif & Fatma, Yulia. (2025). Metode deep learning dalam teknologi deepfake: Systematic literature review. *JATI (Jurnal Mahasiswa Teknik Informatika)*, Vol. 9 No. 2.
- Hamzah, Andi. (2019). *Delik-delik tertentu (Speciale Delicten) di dalam KUHP*. Jakarta: Sinar Grafika.

- Harahap, M. Yahya. (2016). *Pembahasan permasalahan dan penerapan KUHP*. Jakarta: Sinar Grafika.
- Kaunang, Agnes Debora Elisabeth. (2024). Menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. *Lex Privatum*, Vol. 13 No. 4.
- Mertokusumo, Sudikno. (2009). *Penemuan hukum*. Yogyakarta: Liberty.
- Mulyadi, Lilik. (2018). *Hukum acara pidana Indonesia: Normatif, teoretis dan permasalahannya*. Bandung: Citra Aditya Bakti.
- Putusan Pengadilan Negeri Gunung Sugih Nomor 124/Pid.B/2025/PN Gns.
- Ratnawati, Faruqy Nailufar & Rosdiana. (2023). Perlindungan konsumen atas penyebaran berita bohong melalui transaksi elektronik. *Jurnal De Jure*, Vol. 15 No. 1.
- Soekanto, Soerjono. (2003). *Pengantar penelitian hukum*. Jakarta: UI Press.
- Soekanto, Soerjono & Mamudji, Sri. (2015). *Penelitian hukum normatif*. Jakarta: Rajawali Pers.
- Soesilo, R. (1996). *Kitab Undang-Undang Hukum Pidana serta komentar-komentarnya*. Bogor: Politeia.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.