PENEGAKAN HUKUM TINDAK PIDANA PENIPUAN MENGGUNAKAN *ARTIFICIAL INTELLIGENCE* (*DEEPFAKE*)[1]

Oleh: Tesalonika Lengkey[2]
Hervian Rumengan[3]
Diana Rondonuwu[4]

ABSTRAK

Penelitian ini bertujuan untuk mengetahui bagaimana peraturan hukum tindak pidana penipuan menggunakan *artificial intelligence deepfake* dan bagaimana penegakan hukum terhadap pelaku tindak pidana penipuan menggunakan *artificial intelligence deepfake*, dengan metode penelitian yuridis normatif disimpulkan: 1. Pengaturan hukum tindak pidana menggunakan *deepfake* dalam hukum positif Indonesia, yaitu melalui Pasal 35 juncto. Pasal 51 ayat (1) Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP). Dalam hal ini, Pasal 35 juncto Pasal 51 ayat (1) UU ITE berkedudukan sebagai *lex specialis*, sedangkan Pasal 492 KUHP merupakan *lex generalis*. 2. Penegakan hukum tindak pidana penipuan menggunakan *deepfake* berdasarkan Putusan Pengadilan Negeri Pekalongan Nomor 82/Pid.Sus/2025/PN Pkl dilakukan melalui penerapan Pasal 35 juncto Pasal 51 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik sebagai *lex specialis* dibandingkan KUHP sebagai *lex generalis*.

Kata kunci: *Penegakan Hukum*, *Tindak Pidana Penipuan*, *Artificial Intelligence*, *Deepfake*.

PENDAHULUAN

A. Latar Belakang

Di era digital saat ini, perkembangan Teknologi Informasi dan Komunikasi telah berkembang pesat. Teknologi tidak hanya menjadi fasilitas pendukung dalam kegiatan sehari-hari manusia, melainkan telah terintegrasi dalam berbagai aspek kehidupan manusia, termasuk bidang pendidikan, kesehatan, sosial, ekonomi, budaya dan hukum.[5] Hasil dari perkembangan Teknologi Informasi dan Komunikasi yang sangat berpengaruh saat ini adalah *Artificial Intelligence* (selanjutnya disingkat AI) atau Kecerdasan Buatan. Seiring dengan pesatnya perkembangan teknologi digital, AI tidak selalu memberikan dampak positif.

Teknologi AI yang sering disalahgunakan adalah teknologi *deepfake*. Teknologi *deepfake* pada awalnya memberikan berbagai kontribusi positif dalam berbagai sektor, khususnya industri hiburan, seperti produksi film dan pengembangan kreativitas digital melalui media sosial maupun media penyiaran televisi. Namun, keberadaan teknologi ini juga membuka peluang terjadinya penyalahgunaan yang berpotensi menimbulkan kerugian bagi individu maupun masyarakat.[6]

Indonesia belum memiliki peraturan perundang-undangan yang secara khusus mengatur mengenai AI, maupun *deepfake*. Penanganan penyalahgunaan teknologi AI, khususnya *deepfake* dalam tindak pidana penipuan masih menggunakan peraturan perundang-undangan yang berlaku saat ini, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP).

B. Rumusan Masalah

1. Bagaimana pengaturan hukum tindak pidana penipuan menggunakan *Artificial Intelligence Deepfake*?
2. Bagaimana penegakan hukum terhadap pelaku tindak pidana penipuan menggunakan teknologi *Artificial Intelligence Deepfake*?

C. Metode Penelitian

Metode penelitian yang digunakan dalam penulisan skripsi ini adalah penelitian hukum normatif. Penelitian normatif yaitu penelitian hukum yang mengacu pada norma-norma, kaidah dan doktrin yang terdapat dalam peraturan perundang-undangan. Instrumen penelitian hukum normatif dilakukan dengan menganalisa bahan hukum primer, sekunder dan tersier yang berkaitan dengan topik penelitian penulis, yaitu sebagai berikut:

1. Bahan Hukum Primer, yaitu bahan-bahan hukum yang mengikat, yang bersumber pada

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 220711010132
[3] Fakultas Hukum Unsrat, Doktor Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] Agus Wibowo & Sri Yulianingsih, *Hukum Teknologi Informasi*. Semarang: Yayasan Prima Agus Teknik, 2025, hlm. 3.
[6] *Ibid*.

FAKULTAS HUKUM UNSRAT 2026

ketentuan peraturan perundang-undangan. Peraturan perundang- undangan yang digunakan dalam penelitian ini yaitu Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, dan Undang-Undang No.1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
2. Bahan Hukum Sekunder, yaitu bahan hukum yang memberikan penjelasan mengenai bahan hukum primer, berupa literatur-literatur atau kepustakaan lainnya yang membantu penyusunan penelitian ini.
3. Bahan Hukum Tersier, yaitu bahan hukum yang menjadi penunjang bagi bahan hukum primer maupun sekunder, berupa penjelajahan secara dalam jaringan (daring) melalui website ataupun tulisan-tulisan didalam jaringan tersebut.

BAB III
PEMBAHASAN

A. Pengaturan Hukum Tindak Pidana Penipuan Menggunakan *Artificial Intelligence Deepfake*

Perkembangan teknologi AI telah membawa perubahan besar dalam kehidupan masyarakat, termasuk dalam perkembangan kejahatan di ruang digital yang juga menimbulkan tantangan baru dalam penegakan hukum. Dalam sistem hukum positif Indonesia, belum terdapat ketentuan yang secara eksplisit mengatur tentang *deepfake*. Namun demikian, ketentuan dalam peraturan perundang-undangan saat ini dapat diterapkan untuk menjerat pelaku penyalahgunaan teknologi *deepfake* khususnya dalam konteks penipuan. Pengaturan tersebut antara lain, Kitab Undang-Undang Hukum Pidana sebagai *lex generalis*, serta Undang-Undang Informasi dan Transaksi Elektronik sebagai *lex specialis*.

1. Pasal 35 jo. Pasal 51 ayat (1) Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah kedua kalinya menjadi Undang-Undang No 1 Tahun 2024 tentang Informasi Elektronik (*Lex Specialis*)

Undang-Undang No. 11 Tahun 2008 sebagaimana telah diubah kedua kalinya menjadi Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) pada umumnya mengatur segala kejahatan yang dilakukan menggunakan media elektronik.

a. Pasal 35 UU ITE melarang: "*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*".[7]

b. Pasal 51 ayat (1) UU ITE menyatakan bahwa "*Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)*".[8]

Tindak pidana yang dilakukan dengan menggunakan teknologi *deepfake* pada dasarnya memenuhi unsur-unsur sebagaimana diatur dalam Pasal 35 UU ITE, yaitu:

a. Unsur Subjektif

1) Unsur "Setiap Orang", menunjuk pada setiap subjek hukum yang dapat dimintai pertanggungjawaban pidana, baik orang perseorangan maupun korporasi sebagai badan hukum. Subjek hukum tersebut harus memiliki kemampuan untuk mempertanggungjawabkan perbuatannya secara pidana, sehingga dapat dikenai sanksi apabila terbukti memenuhi unsur-unsur tindak pidana.

2) Unsur "Dengan Sengaja", unsur ini terpenuhi apabila pelaku secara sadar dan atas kehendaknya sendiri melakukan pembuatan, penyuntingan, maupun penyebaran konten *deepfake*. Pelaku mengetahui serta menghendaki bahwa konten hasil rekayasa tersebut akan dipercaya sebagai informasi yang benar sehingga berpotensi menyesatkan atau memperdaya masyarakat.

---

[7] Indonesia, Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 35.

[8] Indonesia, Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) Pasal 51 ayat (1).

b. Unsur Objektif

1) Unsur "Tanpa Hak atau Melawan Hukum", unsur ini terpenuhi apabila perbuatan dilakukan tanpa adanya hak, kewenangan, atau persetujuan dari pihak yang identitas visual maupun audionya direkayasa, baik pejabat negara, tokoh publik, maupun masyarakat umum. Selain itu, perbuatan tersebut juga bertentangan dengan ketentuan peraturan perundang-undangan dan prinsip-prinsip hukum yang berlaku.

2) Unsur "Melakukan Manipulasi, Penciptaan, Perubahan, Penghilangan, atau Perusakan Informasi Elektronik dan/atau Dokumen Elektronik", unsur ini tercermin dalam tindakan pelaku yang memanfaatkan teknologi AI untuk merekayasa informasi elektronik atau dokumen elektronik, seperti mengubah wajah, suara, ekspresi, maupun gerakan seseorang sehingga menghasilkan konten digital yang tampak menyerupai aslinya. Rekayasa tersebut menghasilkan informasi elektronik palsu yang memiliki tingkat kemiripan tinggi dengan objek sebenarnya sehingga berpotensi menimbulkan kesan bahwa informasi tersebut merupakan data yang autentik.

c. Unsur Maksud atau Tujuan

1) Unsur "Dengan Tujuan Agar Dianggap Seolah-Olah Data yang Autentik", unsur ini menghendaki adanya kehendak pelaku agar informasi elektronik atau dokumen elektronik hasil manipulasi dipercaya sebagai data yang asli atau autentik. Dengan adanya kesan keaslian tersebut, korban terdorong untuk mempercayai informasi yang disampaikan, sehingga bersedia menyerahkan sejumlah uang, data pribadi, atau bentuk keuntungan lain yang diinginkan oleh pelaku.

Ketentuan Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dikualifikasikan sebagai delik formil, yaitu tindak pidana yang dianggap telah terpenuhi apabila pelaku melakukan perbuatan yang dilarang oleh undang-undang, tanpa mensyaratkan timbulnya akibat tertentu sebagai unsur delik.[9]

2. Pasal 492 Undang-Undang No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (*Lex Generalis*)

Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP) merupakan ketentuan umum yang mengatur mengenai tindak pidana penipuan. Meskipun ketentuan tersebut tidak secara khusus mengatur mengenai *deepfake*, norma yang terkandung di dalamnya tetap dapat diterapkan terhadap tindak pidana penipuan yang dilakukan dengan memanfaatkan teknologi tersebut, sepanjang seluruh unsur delik penipuan terpenuhi. Dalam konteks ini, teknologi *deepfake* hanya berfungsi sebagai sarana untuk melakukan penipuan, sedangkan esensi perbuatannya tetap berupa tindakan memperdaya orang lain demi memperoleh keuntungan secara melawan hukum.

Pasal 492 KUHP menyatakan 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, dipidana karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori V*".[10] Unsur-unsur penipuan dalam pasal ini mencakup: [11]

a. Unsur "Setiap orang", merujuk kepada setiap subjek hukum yang dapat dimintai pertanggungjawaban pidana, baik orang perseorangan maupun korporasi. Dalam tindak pidana penipuan berbasis *deepfake*, pelaku yang secara sadar membuat, menguasai, atau menyebarluaskan konten *deepfake* untuk melakukan penipuan merupakan subjek hukum yang memenuhi unsur ini dan dapat dimintai pertanggungjawaban pidana sesuai dengan ketentuan yang berlaku.

---

[9] Nikles Denny Ardiansyah, dkk., *Jurnal Reformasi Hukum: Cogito Ergo Sum*, Vol. 7, No. 2, 2024, hlm. 20

[10] Indonesia, Undang-Undang No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP) Pasal 492.

[11] *Ibid.*

b. Unsur "Dengan Maksud Menguntungkan Diri Sendiri atau Orang Lain Secara Melawan Hukum", menghendaki adanya tujuan dari pelaku untuk memperoleh keuntungan yang bertentangan dengan hukum. Pada tindak pidana penipuan berbasis *deepfake*, keuntungan tersebut umumnya berupa uang, harta benda, maupun manfaat ekonomi lainnya yang diperoleh melalui penyebaran video *deepfake*. Keuntungan tersebut diperoleh dengan cara melawan hukum karena didasarkan pada tipu daya yang mengakibatkan korban menyerahkan harta bendanya secara sukarela.

c. Unsur "Menggunakan Nama Palsu, Martabat Palsu, Tipu Muslihat, atau Rangkaian Kebohongan", merupakan inti dari tindak pidana penipuan. Dalam modus *deepfake*, pelaku memanfaatkan teknologi AI untuk merekayasa wajah, suara, maupun gerakan seseorang sehingga tampak seolah-olah tokoh yang ditampilkan benar-benar menyampaikan informasi tertentu. Penggunaan identitas digital palsu tersebut merupakan bentuk tipu muslihat dan rangkaian kebohongan yang bertujuan membangun kepercayaan korban.

d. Unsur "Menggerakkan Orang Lain untuk Menyerahkan Barang, Memberi Utang, atau Menghapuskan Piutang". Tindak pidana penipuan merupakan delik materiil, sehingga unsur ini baru terpenuhi apabila tipu muslihat yang dilakukan pelaku benar-benar menggerakkan korban untuk menyerahkan barang, mentransfer sejumlah uang, memberikan pinjaman, atau menghapuskan piutang.

Pasal 492 KUHP dapat diterapkan terhadap tindak pidana penipuan berbasis *deepfake* karena seluruh unsur delik penipuan pada dasarnya dapat dipenuhi. Namun demikian, mengingat *deepfake* merupakan bentuk manipulasi terhadap Informasi Elektronik dan/atau Dokumen Elektronik, maka perbuatan tersebut juga memenuhi ketentuan Pasal 35 Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Oleh karena itu, dalam penanganan tindak pidana penipuan yang menggunakan teknologi *deepfake*, pasal 492 KUHP berkedudukan sebagai *lex generalis*, sedangkan pasal 35 juncto pasal 51 ayat (1) UU ITE merupakan *lex specialis* yang secara khusus mengatur manipulasi informasi elektronik.

Berdasarkan asas *lex specialis derogat legi generali*, apabila suatu perbuatan memenuhi unsur dalam kedua ketentuan tersebut, maka ketentuan dalam UU ITE pada prinsipnya didahulukan penerapannya karena mengatur secara lebih spesifik mengenai perbuatan manipulasi informasi elektronik sebagai sarana terjadinya tindak pidana penipuan.

3. Tata Cara/Mekanisme Penegakan Hukum Tindak Pidana Menggunakan *Deepfake* menurut KUHAP

Penegakan hukum terhadap tindak pidana penipuan menggunakan *deepfake* tidak hanya ditentukan oleh adanya ketentuan pidana yang mengatur perbuatan tersebut, tetapi juga oleh tata cara yang dilaksanakan sesuai dengan ketentuan Undang-Undang No. 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Undang-Undang Informasi dan Transaksi Elektronik (ITE). Tata cara peradilan pidana merupakan rangkaian proses penegakan hukum yang dimulai dari penyelidikan, penyidikan, penuntutan, hingga pemeriksaan di persidangan, sebagai upaya untuk menegakkan hukum dan memberikan kepastian hukum terhadap suatu tindak pidana.

Proses penegakan hukum diawali dengan adanya laporan dari masyarakat terkait dugaan tindak pidana. Ketika terjadi tindak pidana berbasis *deepfake*, masyarakat dapat melapor kepada Kepolisian Negara Republik Indonesia maupun Kementerian Komunikasi dan Digital Republik Indonesia.[12]

a. Tahap Penyelidikan

Menurut pasal 1 angka 8 KUHAP, penyelidikan adalah serangkaian tindakan penyelidik untuk mencari dan menemukan peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan.[13] Tahap penyelidikan bertujuan untuk menemukan serta memastikan adanya suatu peristiwa yang diduga sebagai tindak pidana.

Dalam perkara penipuan berbasis *deepfake*, penyelidik melakukan upaya pengumpulan informasi awal yang berkaitan dengan konten digital, identitas, dan rangkaian peristiwa berdasarkan keterangan yang diberikan

[12] Agus Wibowo & Sri Yulianingsih, *op.cit*, hlm. 55

[13] Undang-Undang No. 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana Pasal 1 angka 8.

oleh korban.[14] Setelah ditemukan adanya dugaan tindak pidana, proses penegakan hukum dilanjutkan ke tahap penyidikan.

b. Tahap Penyidikan

Menurut pasal 1 angka 5 KUHAP, penyidikan adalah serangkaian tindakan Penyidik untuk mencari dan mengumpulkan alat bukti guna membuat terang tindak pidana, serta menemukan tersangka.[15] Tahap penyidikan bertujuan untuk mengumpulkan alat bukti guna menemukan pihak yang diduga sebagai pelaku. Dalam perkara tindak pidana siber, penyidik tidak hanya mengumpulkan alat bukti yang bersifat konvensional, tetapi juga alat bukti elektronik yang berkaitan dengan perbuatan pidana yang dilakukan.[16] Bukti elektronik dan hasil analisis forensik digital memiliki peranan penting dalam membuktikan adanya manipulasi digital yang dilakukan menggunakan teknologi AI.

c. Tahap Penuntutan

Menurut pasal 1 angka 11 KUHAP, penuntutan adalah tindakan Penuntut Umum untuk melimpahkan perkara pidana ke pengadilan negeri yang berwenang untuk diperiksa dan diputus oleh hakim di sidang pengadilan.[17] Setelah proses penyidikan dinyatakan lengkap, berkas perkara dilimpahkan kepada Kejaksaan Republik Indonesia untuk dilakukan penuntutan. Jaksa memiliki kedudukan yang penting dalam menilai terpenuhinya kecukupan alat bukti serta menyusun surat dakwaan yang merupakan dasar bagi hakim dalam memeriksa dan mengadili suatu perkara pidana.[18]

d. Tahap Pemeriksaan di Persidangan

Pada tahap ini, majelis hakim melakukan penilaian terhadap alat bukti yang diajukan oleh penuntut umum guna menentukan terpenuhinya unsur-unsur tindak pidana serta adanya kesalahan yang dapat dipertanggungjawabkan kepada terdakwa.[19] Dalam kasus penipuan deepfake, bukti elektronik memiliki peranan penting dalam membuktikan adanya manipulasi digital yang dilakukan melalui teknologi AI. Berdasarkan hasil pemeriksaan tersebut, pengadilan kemudian menjatuhkan putusan sesuai dengan ketentuan hukum yang berlaku.

B. Penegakan Hukum Tindak Pidana Penipuan Meggunakan *Artificial Intelligence Deepfake*

Perkembangan teknologi AI telah membawa perubahan besar dalam kehidupan masyarakat, termasuk dalam perkembangan kejahatan di ruang digital yang menimbulkan tantangan baru dalam penegakan hukum, khususnya dalam penegakan hukum kejahatan siber (selanjutnya disebut *cybercrime*). Menurut Agus Rahardjo (2002), *cybercrime* merupakan segala kejahatan/perilaku ilegal yang dilakukan oleh seseorang, sekelompok orang atau korporasi dengan menggunakan jaringan internet dan juga perangkat digital lainnya sebagai alat utama.[20] Sebagai bentuk kejahatan berbasis teknologi tinggi (*high-tech crime*) yang memiliki karakter lintas negara (*transnational/transborder*), penegakan hukum terhadap *cybercrime* memerlukan dukungan pendekatan teknologi guna mengimbangi perkembangan metode dan sarana yang digunakan oleh pelaku.[21]

Tindak pidana berbasis *deepfake* memiliki keterkaitan yang erat dengan *cybercrime* dikarenakan *deepfake* merupakan salah satu bentuk kejahatan berbasis teknologi digital yang dilakukan melalui pemanfaatan sistem komputer dan jaringan internet. *Deepfake* sebagai bentuk *cybercrime* terlihat dari penggunaan internet dan media digital sebagai sarana utama penyebaran konten *deepfake*, seperti melalui media sosial, aplikasi komunikasi, maupun platform digital lainnya. Selain itu, *deepfake* juga berkaitan dengan karakteristik *cybercrime* yang bersifat lintas batas (*transnasional/transborder*), anonim, serta sulit dideteksi. Kondisi ini menyebabkan proses penegakan hukum terhadap tindak pidana

[14] Sarda dan Dewi Asri Puanandini, "Penegakan Hukum Terhadap Tindak Pidana Penipuan Melalui Media Telepon Dalam Perspektif Hukum Telematika", Al-Zayn: Jurnal Ilmu Sosial & Hukum, 2026, Vol. 4, No. 1, hlm. 4600.

[15] Undang-Undang No. 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana Pasal 1 angka 5.

[16] Sarda dan Dewi Asri Puanandini, *op.cit,* hlm. 4600-4601

[17] Undang-Undang No. 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana Pasal 1 angka 11.

[18] Sarda dan Dewi Asri Puanandini, *loc.cit*.

[19] *Ibid.*

[20] Hery Firmansyah, dkk., "Penerapan Kebijakan Digital Dalam Rangka Pencegahan Cyber Crime Ditinjau Dari Undang-Undang Ite", *Seri Seminar Nasional Ke-III Universitas Tarumanagara*, 2021, hlm. 1780.

[21] Barda Nawawi Arief, *Tindak Pidana Mayantara (Perkembangan Kajian Cyber Crime di Indonesia)*. Jakarta: Raja Grafindo, 2007, hlm.90.

penipuan berbasis *deepfake* menjadi lebih kompleks.

Penegakan hukum terhadap tindak pidana yang memanfaatkan teknologi *deepfake* pada dasarnya dapat dilakukan melalui dua pendekatan, yaitu upaya penal (represif) dan upaya non-penal (preventif). Upaya penal merupakan bentuk penegakan hukum yang dilakukan setelah terjadinya suatu tindak pidana melalui penerapan ketentuan hukum pidana terhadap pelaku. Sementara itu, upaya non-penal fokus pada pencegahan terjadinya tindak pidana melalui berbagai langkah preventif. Penerapan upaya penal dalam penegakan hukum terhadap tindak pidana berbasis deepfake dapat dianalisis melalui Putusan Pengadilan Negeri Pekalongan Nomor 82/Pid.Sus/2025/PN Pkl, yang menjadi salah satu contoh penegakan hukum terhadap tindak pidana penipuan menggunakan teknologi *deepfake*.

1. Putusan Nomor 82/Pid.Sus/2025/PN Pkl

Pada bulan Desember 2024 Terdakwa Juanda Saputra Bin Abdul Malik mengunduh video *deepfake* yang menampilkan wajah Presiden Prabowo Subianto dan Menteri Keuangan Sri Mulyani. Video tersebut diperoleh dari unggahan akun media sosial Instagram milik pihak lain yang tidak diketahui identitasnya melalui mesin pencarian Google. Selanjutnya, terdakwa mengunggah kembali video tersebut pada akun Instagram miliknya dengan nama pengguna "indoberbagi2025". Dalam video tersebut ditampilkan seolah-olah Presiden Prabowo Subianto dan Menteri Keuangan Sri Mulyani sedang menyampaikan informasi mengenai program resmi pemerintah berupa bantuan pelunasan utang dan pemberian modal usaha kepada masyarakat. Melalui unggahan tersebut, calon korban diarahkan untuk menghubungi nomor WhatsApp milik terdakwa yang dicantumkan pada unggahan. Setelah menghubungi nomor tersebut, korban diminta mengisi formulir yang berisi data identitas pribadi serta mentransfer sejumlah uang yang diklaim sebagai biaya administrasi dan biaya pencairan bantuan ke rekening Bank Central Asia (BCA) yang sebelumnya telah dibeli dan dikuasai oleh terdakwa.[22]

Terdakwa menggunakan video deepfake sebagai sarana untuk melakukan tindak pidana penipuan karena beranggapan bahwa teknologi tersebut masih belum banyak dipahami oleh masyarakat. Selain itu, penggunaan video yang menampilkan pejabat negara, yaitu Presiden Prabowo Subianto dan Menteri Keuangan Sri Mulyani, bertujuan untuk meningkatkan kepercayaan calon korban terhadap informasi yang disampaikan sehingga mereka terdorong untuk mengikuti instruksi yang diberikan oleh terdakwa. Terdakwa melakukan perbuatannya secara seorang diri. Akibat perbuatan tersebut, sekitar 30 orang menjadi korban dengan total keuntungan yang diperoleh terdakwa diperkirakan mencapai Rp30.000.000. Beberapa korban yang telah diperiksa dalam persidangan antara lain Saksi Hakimah bersama suaminya, Sulaiman, yang mengalami kerugian sebesar Rp5.900.000, Saksi Perri Sampeallo yang mengalami kerugian sebesar Rp250.000, serta Saksi Liem Wen Jiang yang mengalami kerugian sebesar Rp300.000.[23]

Berdasarkan Putusan Pengadilan Negeri Pekalongan, Majelis Hakim menyatakan bahwa Terdakwa Juanda Saputra bin Abdul Malik telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana dengan sengaja dan tanpa hak melakukan manipulasi Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah sebagai data yang autentik. Perbuatan tersebut dikualifikasikan sebagai tindak pidana sebagaimana diatur dalam Pasal 35 juncto Pasal 51 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Atas perbuatan tersebut, Majelis Hakim menjatuhkan pidana kepada terdakwa dengan pidana penjara selama 1 (satu) tahun 10 (sepuluh) bulan dan denda sebesar Rp10.000.000,00 (sepuluh juta rupiah) dengan ketentuan apabila denda tersebut tidak dibayarkan, maka diganti dengan pidana kurungan selama 3 (tiga) bulan. Masa penangkapan dan penahanan yang telah dijalani terdakwa diperhitungkan seluruhnya sebagai pengurang masa pidana yang dijatuhkan. Barang bukti yang digunakan dalam pelaksanaan tindak pidana, berupa beberapa unit telepon seluler dan kartu Anjungan Tunai Mandiri (ATM), Majelis Hakim menetapkan agar barang bukti tersebut dirampas untuk dimusnahkan atau

[22] Direktori Putusan Makamah Agung Republik Indonesia, Putusan Nomor 82/Pid.Sus/2025/PN Pkl. https://putusan3.mahkamahagung.go.id (diakses 20 Juli 2026)

[23] *Ibid.*

dirampas untuk negara sesuai dengan amar putusan.[24]

Pertimbangan hukum Majelis Hakim dalam perkara ini didasarkan pada terpenuhinya unsur-unsur tindak pidana yang diatur dalam Pasal 35 juncto Pasal 51 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang meliputi:

a. Unsur "Setiap Orang"

Majelis Hakim menilai bahwa Terdakwa Juanda Saputra bin Abdul Malik merupakan subjek hukum yang cakap untuk mempertanggungjawabkan perbuatannya. Berdasarkan fakta yang terungkap dalam persidangan, Terdakwa berusia 25 tahun serta berada dalam kondisi sehat jasmani dan rohani. Selain itu, tidak ditemukan adanya alasan pembenar maupun alasan pemaaf yang dapat menghapus sifat melawan hukum atau kesalahan Terdakwa, sehingga dapat dimintai pertanggungjawaban pidana atas perbuatannya.

b. Unsur "Dengan Sengaja dan Tanpa Hak atau Melawan Hukum"

Secara doktrinal, unsur "dengan sengaja" dimaknai sebagai adanya kehendak (*willens*) dan pengetahuan (*wetens*) dari pelaku terhadap perbuatan yang dilakukannya. Dalam perkara ini, unsur kesengajaan terbukti dari serangkaian tindakan yang dilakukan oleh Terdakwa secara sadar dan terencana, yaitu bergabung dalam grup yang membahas modus penipuan menggunakan AI, mengunduh video *deepfake*, mengunggah video tersebut melalui media sosial, serta menyediakan rekening yang digunakan untuk menerima dana dari para korban. Rangkaian perbuatan tersebut menunjukkan bahwa Terdakwa mengetahui dan menghendaki akibat yang ditimbulkan dari tindakannya, yaitu memperoleh keuntungan dengan memanfaatkan video *deepfake* sebagai sarana penipuan. Unsur "tanpa hak atau melawan hukum" juga telah terpenuhi karena Terdakwa tidak memiliki hak, izin, maupun kewenangan untuk menggunakan identitas, citra, maupun video yang menampilkan tokoh-tokoh publik dalam unggahannya. Selain itu, penggunaan video *deepfake* tersebut dilakukan untuk menciptakan kesan seolah-olah informasi yang disampaikan berasal dari pihak yang sebenarnya, sehingga menimbulkan kepercayaan masyarakat dan mendorong korban untuk menyerahkan sejumlah uang. Dengan demikian, perbuatan Terdakwa bertentangan dengan ketentuan hukum yang berlaku dan dilakukan dengan tujuan memperoleh keuntungan secara melawan hukum melalui tindakan penipuan.

c. Unsur "Melakukan Manipulasi, Penciptaan, Perubahan, Penghilangan, Pengrusakan Informasi/Dokumen Elektronik"

Penambahan narasi mengenai bantuan pelunasan utang, *caption* promosi yang bersifat menyesatkan, serta pencantuman nomor WhatsApp pribadi pada video *deepfake* menunjukkan adanya tindakan aktif yang dilakukan oleh Terdakwa untuk mengubah dan memanipulasi Informasi Elektronik. Perbuatan tersebut mengakibatkan video tersebut memiliki kesan sebagai informasi yang autentik sehingga berpotensi menimbulkan kepercayaan masyarakat terhadap isi informasi yang disampaikan.

d. Unsur "Dengan Tujuan Agar Informasi/Dokumen Elektronik Tersebut Dianggap Seolah-Olah Data yang Otentik"

Unsur ini merupakan aspek yang paling mendasar dalam tindak pidana yang memanfaatkan *deepfake*. Berdasarkan pertimbangan Majelis Hakim, Terdakwa secara sengaja menggunakan wajah dan suara hasil manipulasi yang menyerupai Presiden Republik Indonesia Prabowo Subianto dan Menteri Keuangan Sri Mulyani untuk membangun kepercayaan masyarakat terhadap informasi yang disampaikan. Penggunaan identitas tokoh publik tersebut dimaksudkan agar video yang diunggah terlihat seolah-olah berasal dari sumber yang resmi dan autentik, sehingga korban mempercayai adanya program bantuan pemerintah dan terdorong untuk mengirimkan sejumlah uang sesuai dengan instruksi yang diberikan oleh Terdakwa.

Penerapan Pasal 35 juncto Pasal 51 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik oleh Majelis Hakim dalam perkara ini dinilai telah sesuai dengan karakteristik perbuatan yang dilakukan oleh terdakwa. Meskipun perbuatan tersebut pada dasarnya memiliki keterkaitan dengan tindak pidana penipuan sebagaimana diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP),

[24] *Ibid.*

penggunaan ketentuan dalam UU ITE lebih tepat diterapkan mengingat tindak pidana dilakukan melalui manipulasi Informasi Elektronik dengan memanfaatkan *deepfake*.

Dalam perspektif hukum pidana, kondisi tersebut menunjukkan adanya hubungan antara ketentuan umum dan ketentuan khusus. Penyelesaiannya dilakukan melalui penerapan asas *lex specialis derogat legi generali*, yaitu ketentuan yang bersifat khusus mengesampingkan ketentuan yang bersifat umum. Oleh karena itu, ketentuan Pasal 35 juncto Pasal 51 ayat (1) UU ITE menjadi dasar hukum yang lebih relevan dibandingkan Pasal 378 KUHP karena secara khusus mengatur perbuatan manipulasi Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar informasi tersebut dianggap sebagai data yang autentik. Selain memberikan dasar hukum yang lebih spesifik terhadap penyalahgunaan teknologi digital, ketentuan Pasal 35 UU ITE juga mencerminkan karakteristik tindak pidana yang dilakukan melalui manipulasi data elektronik, termasuk penggunaan teknologi *deepfake*. Ketentuan tersebut tidak hanya memberikan kepastian hukum terhadap bentuk-bentuk kejahatan yang memanfaatkan media elektronik, tetapi juga memberikan perlindungan hukum terhadap keaslian dan integritas Informasi Elektronik sebagai objek yang dilindungi oleh UU ITE.

Dalam kaitan dengan kasus *deepfake* yang melibatkan Juanda Saputra bin Abdul Malik, yang menggunakan Pasal 35 UU ITE, dimana bunyi dari Pasal tersebut:[25]

"*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.*"

Dipasangkan secara berlapis dengan Pasal 51 ayat (1) UU ITE dimana bunyi dari Pasal tersebut adalah:[26]

"Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)."

Putusan Pengadilan Negeri Pekalongan Nomor 82/Pid.Sus/2025/PN Pkl terhadap tindak pidana penipuan menggunakan *deepfake* menunjukkan bahwa proses penegakan hukum telah dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Penulis mendapati bahwa Putusan jauh dibawah nilai maksimal yang di amanatkan oleh Undang-Undang, yaitu hanya 1 (satu) tahun 10 (sepuluh) bulan, dengan denda sebesar Rp. 10.000.000 (sepuluh juta rupiah).

Penepatan putusan yang sedemikian ini menunjukan adanya peringanan hukuman yang diterapkan oleh Hakim dengan mempertimbangkan berbagai faktor-faktor sebagaimana pembelaan dari kuasa hukum terdakwa. yaitu Majelis Hakim memberikan putusan yang seringan-ringannya dengan pertimbangan karena terdakwa tulang punggung keluarga, orang tua terdakwa tidak bekerja, dan ayah terdakwa sedang sakit, selain itu terdakwa merasa menyesal dan berjanji tidak akan mengulangi lagi perbuatannya.

Berdasarkan uraian tersebut, dapat dipahami bahwa penegakan hukum terhadap tindak pidana penipuan yang memanfaatkan teknologi *deepfake* dalam Putusan Pengadilan Negeri Pekalongan Nomor 82/Pid.Sus/2025/PN Pkl menunjukkan bahwa ketentuan Pasal 35 juncto Pasal 51 ayat (1) Undang-Undang No. 11 Tahun 2008 sebagaimana telah diubah kedua kalinya dengan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dapat diterapkan sebagai dasar pertanggungjawaban pidana terhadap tindak pidana yang melibatkan *deepfake*.

Majelis Hakim menilai seluruh unsur tindak pidana telah terpenuhi sehingga terdakwa dinyatakan bersalah atas manipulasi Informasi Elektronik yang bertujuan agar informasi tersebut dianggap sebagai data yang autentik. Penerapan ketentuan tersebut mencerminkan penggunaan asas *lex specialis derogat legi generali*, sehingga UU ITE menjadi dasar hukum yang lebih tepat dibandingkan ketentuan penipuan dalam KUHP. Dengan demikian, putusan ini menunjukkan bahwa sistem hukum pidana Indonesia memiliki landasan normatif yang dapat digunakan untuk menindak pelaku penipuan yang memanfaatkan teknologi *deepfake* serta memberikan kepastian hukum dalam penanganan kejahatan berbasis *deepfake*.

[25] Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 35.

[26] Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 51 ayat (1).

2. Upaya Penegakan Hukum Non-penal (Preventif)

Upaya penegakan hukum tindak pidana berbasis *deepfake* tidak hanya dilakukan melalui upaya penal (penerapan hukum pidana) namun juga harus dilakukan upaya penal (preventif). Upaya penegakan hukum melalui jalur non-penal berfokus pada aspek pencegahan terhadap terjadinya tindak pidana. Sasaran utama pendekatan non-penal adalah mengatasi berbagai faktor yang berpotensi mendukung atau mendorong terjadinya kejahatan. Faktor-faktor tersebut umumnya berkaitan dengan permasalahan maupun kondisi sosial yang baik secara langsung maupun tidak langsung, dapat menjadi penyebab munculnya serta berkembangnya perilaku kriminal dalam masyarakat.[27]

Penanggulangan tindak pidana penipuan berbasis *deepfake* secara non-penal harus dilakukan secara strategis sistematis seperti yang dikemukakan oleh Muladi, yaitu:

a. Perlu dirumuskan suatu undang-undang payung (*umbrella act*) yang secara komprehensif mengatur kebijakan di bidang AI terlebih khusus *deepfake*, baik yang diselenggarakan melalui media cetak, media penyiaran, maupun media siber. Kehadiran regulasi tersebut bertujuan untuk menciptakan kerangka hukum yang terpadu dalam menghadapi berbagai perkembangan AI.[28]

b. Perlu menyusun kode etik, kode perilaku, dan pedoman praktik, mengenai penggunaan teknologi AI yang disusun secara profesional. Instrumen tersebut berfungsi sebagai pedoman bagi pengguna teknologi AI agar pemanfaatan teknologi tersebut dilakukan secara bertanggung jawab dan sesuai dengan norma hukum serta etika yang berlaku.[29]

c. Perlu kerjasama yang sinergis antara berbagai pihak yang berkepentingan, termasuk pemerintah, aparat penegak hukum, akademisi, masyarakat, dan sektor industri teknologi. Kerja sama tersebut diarahkan pada pengembangan teknologi pencegahan (*preventive technology*) yang mampu mendeteksi, mengantisipasi, dan meminimalkan risiko terjadinya tindak pidana berbasis *deepfake*.[30]

Karakteristik *deepfake* yang terus berkembang seiring kemajuan teknologi, memerlukan langkah-langkah preventif yang dilakukan secara berkelanjutan. Beberapa upaya yang dapat diterapkan antara lain:[31]

a. Meningkatkan kesadaran (*awareness*) masyakarat terhadap berbagai bentuk ancaman tindak pidana berbasis *deepfake* khususnya dalam konteks penipuan yang berpotensi mengganggu keamanan informasi dan menimbulkan kerugian. Selain itu, organisasi perlu menerapkan standar keamanan informasi siber secara menyeluruh sebagai bentuk perlindungan terhadap sistem dan data yang dimiliki.

b. Meningkatkan dan mengembangkan kapasitas sumber daya manusia melalui pelatihan dan pendidikan mengenai keamanan siber yang dilakukan secara berkala agar individu yang terlibat memiliki kompetensi yang memadai dalam menghadapi berbagai ancaman digital.

c. Menerapkan arsitektur sistem dan layanan yang aman serta melakukan pembaruan (*update*) secara berkala.

d. Memiliki kemampuan dalam melakukan pencegahan, mitigasi, remediasi, serta audit keamanan sistem secara berkala.

Dengan demikian, upaya-upaya tersebut bertujuan untuk mengidentifikasi potensi ancaman sejak dini, meminimalkan dampak yang ditimbulkan apabila terjadi tindak pidana penipuan berbasis *deepfake*, serta memastikan efektivitas sistem keamanan yang telah diterapkan.

BAB IV
PENUTUP

A. Kesimpulan

1. Pengaturan hukum tindak pidana menggunakan *deepfake* dalam hukum positif Indonesia, yaitu melalui Pasal 35 juncto. Pasal

[27] Budi Suhariyanto, *loc.cit.*

[28] Widodo, *Memerangi Cybercrime (Karakteristik, motivasi, dan Strategi Penanganannya dalam Perspektif Kriminologi)*. Yogyakarta: Aswaja Pressindo, 2013, hlm. 147.

[29] *Ibid.*

[30] *Ibid.*

[31] Maskun, *Kejahatan Siber (Cyber Crime) Suatu Pengantar*. Jakarta: Kencana Prenada Media Group, 2013, hlm. 95.

51 ayat (1) Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP). Dalam hal ini, Pasal 35 juncto Pasal 51 ayat (1) UU ITE berkedudukan sebagai *lex specialis*, sedangkan Pasal 492 KUHP merupakan *lex generalis*. Oleh karena itu, penerapan Pasal 35 juncto Pasal 51 ayat (1) UU ITE lebih tepat didahulukan berdasarkan asas *lex specialis derogat legi generali*.

2. Penegakan hukum terhadap tindak pidana penipuan menggunakan *deepfake* dalam Putusan Pengadilan Negeri Pekalongan Nomor 82/Pid.Sus/2025/PN Pkl menunjukkan bahwa Majelis Hakim menerapkan Pasal 35 juncto Pasal 51 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik sebagai dasar pertanggungjawaban pidana karena perbuatan terdakwa merupakan manipulasi Informasi Elektronik, sehingga UU ITE diterapkan sebagai *lex specialis* dibandingkan KUHP sebagai *lex generalis*. Terdakwa dijatuhi pidana penjara selama 1 (satu) tahun 10 (sepuluh) bulan dan denda Rp10.000.000,00. (sepuluh juta rupiah) dengan mempertimbangkan keadaan-keadaan yang meringankan terdakwa. Selain melalui pendekatan represif, penanggulangan tindak pidana berbasis deepfake juga perlu didukung oleh pendekatan preventif.

B. Saran

1. Diperlukan pengaturan yang secara khusus mengatur tentang AI terlebih khusus *deepfake*. Meskipun ketentuan dalam UU ITE dapat digunakan sebagai dasar penegakan hukum, pengaturan khusus yang mengatur *deepfake* diperlukan untuk mencegah, memberikan kepastian hukum, memperjelas ruang lingkup perbuatan yang dilarang, serta memberikan perlindungan terhadap masyarakat dari penyalahgunaan *deepfake*.
2. Diperlukan penegakan hukum yang optimal terhadap tindak pidana berbasis *deepfake* melalui peningkatan kapasitas dan pemahaman masyarakat mengenai *deepfake*, serta memperkuat kerja sama dengan pemerintah, penyelenggara platform digital, dan masyarakat dalam upaya pencegahan, deteksi, dan penanggulangan penyalahgunaan teknologi deepfake secara berkelanjutan.

DAFTAR PUSTAKA

Buku:

Arief, Barda Nawawi. 2007. *Tindak Pidana Mayantara (Perkembangan Kajian Cyber Crime di Indonesia)*. Jakarta: RajaGrafindo Persada.

Suhariyanto, Budi. 2013. *Tindak Pidana Teknologi Informasi (cybercrime)*. Jakarta: Rajawali Pers.

Wibowo, Agus dan Sri Yulianingsih. 2025. *Hukum Teknologi Informasi*. Semarang: Yayasan Prima Agus Teknik.

Widodo. 2013. *Memerangi Cybercrime (Karakteristik, Motivasi, dan Strategi Penanganannya dalam Perspektif Kriminologi)*. Yogyakarta: Aswaja Pressindo.

Jurnal/artikel:

Ardiansyah, Nikles Denny, dkk. 2024. *Jurnal Reformasi Hukum: Cogito Ergo Sum*, Vol. 7, No. 2, hlm. 20.

Firmansyah, Hery, dkk. 2021. "Penerapan Kebijakan Digital Dalam Rangka Pencegahan Cyber Crime Ditinjau Dari Undang-Undang Ite". *Seri Seminar Nasional Ke-III Universitas Tarumanagara.*

Sarda dan Dewi Asri Puanandini. 2026. "Penegakan Hukum Terhadap Tindak Pidana Penipuan Melalui Media Telepon Dalam Perspektif Hukum Telematika". *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, Vol. 4, No. 1.

Website:

Direktori Putusan Mahkamah Agung Republik Indonesia. Putusan Nomor 82/Pid.Sus/2025/PN Pkl. https://putusan3.mahkamahagung.go.id (diakses 20 Juli 2026).

Peraturan Perundang-Undangan:

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

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

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

Indonesia. Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana.