



Kekosongan Hukum dalam Menjerat Tindak Pidana Berbasis *Deepfake*: Ancaman Baru dalam Pembuktian

Roihan Hanaan Hanifa
roihanahanaanhanifa22@gmail.com

Sri Astutik
sri.astutik@unitomo.ac.id

Muhammad Yustino Aribawa
yustino@unitomo.ac.id

Sri Sukmana Damayanti
srisukmanad@gmail.com

Abstrak

Artikel ini menyajikan analisis mendalam dan komprehensif mengenai fenomena *deepfake*, manipulasi media sintetik berbasis kecerdasan buatan dan implikasi yuridisnya yang mendisrupsi sistem hukum pidana Indonesia. Di tengah akselerasi teknologi *Generative Adversarial Networks* (GANs) yang memungkinkan penciptaan realitas tiruan dengan tingkat presisi yang nyaris sempurna, sistem hukum positif Indonesia yang masih berpijak pada paradigma konvensional menghadapi ancaman kekosongan norma (*legal vacuum*) yang serius. Penelitian ini menelaah secara kritis instrumen hukum utama, yakni Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Kitab Undang-Undang Hukum Pidana (KUHP) Nasional, dan Undang-Undang Perlindungan Data Pribadi (UU PDP), untuk mengidentifikasi celah regulasi yang gagal menjangkau karakteristik unik *deepfake* sebagai "kebenaran sintetik" yang bersifat generatif, bukan sekadar manipulatif. Temuan studi menunjukkan bahwa frasa "memanipulasi data otentik" dalam Pasal 35 UU ITE mengandung ambiguitas fatal ketika diterapkan pada konten yang diciptakan *ab nihilo* oleh AI. Lebih jauh, laporan ini mengupas ancaman prosedural berupa "Deepfake Defense" atau dividen pembohong, di mana eksistensi teknologi ini dimanfaatkan oleh pelaku kejahatan nyata untuk menyangkal bukti otentik di pengadilan, menciptakan krisis epistemologis dalam pembuktian pidana. Melalui metode penelitian yuridis-normatif dengan pendekatan perbandingan hukum terhadap *Deep Synthesis Provisions* Tiongkok dan *EU AI Act*, laporan ini merekomendasikan urgensi reformasi hukum yang tidak hanya bersifat represif tetapi juga preventif melalui kewajiban transparansi algoritmik dan standarisasi forensik digital nasional yang adaptif.

Kata Kunci: Kekosongan Hukum, *Deepfake*, Pembuktian

A. Latar Belakang

Sejarah peradaban manusia tidak dapat dilepaskan dari upaya untuk merekam realitas. Namun, seiring dengan kemampuan merekam, lahir pula kemampuan untuk memanipulasi. Selama beberapa dekade terakhir, manipulasi konten visual dan audio terbatas pada ranah penyuntingan manual yang memerlukan keahlian teknis tinggi (*high skill*) dan waktu yang lama. Penggunaan perangkat lunak seperti *Adobe Photoshop* atau teknik penyambungan video (*splicing*) konvensional meninggalkan jejak digital atau artefak visual yang relatif mudah dideteksi oleh mata telanjang atau analisis forensik dasar. Dalam konteks hukum, pembuktian terhadap manipulasi semacam ini telah memiliki preseden yang cukup mapan, di mana ahli digital forensik dapat menunjuk ketidaksinkronan piksel atau pencahayaan sebagai bukti rekayasa.¹

Namun, kita kini berada di ambang revolusi teknologi yang mengubah lanskap decepti digital secara fundamental. Revolusi Industri 4.0 dan transisi menuju *Society 5.0* telah memperkenalkan *Artificial Intelligence* (AI) generatif sebagai aktor baru. Teknologi *deepfake*, sebuah istilah yang merupakan gabungan dari "deep learning" dan "fake", bukan sekadar evolusi dari *photoshop*, melainkan sebuah lompatan kuantum. Teknologi ini memanfaatkan arsitektur *Generative Adversarial Networks* (GANs), sebuah sistem yang terdiri dari dua jaringan saraf tiruan yang saling berkompetisi: *Generator* yang bertugas menciptakan konten palsu, dan *Discriminator* yang bertugas mendeteksi kepalsuan tersebut. Melalui jutaan iterasi pelatihan, *Generator* belajar untuk menghasilkan citra, suara, atau video yang begitu realistis hingga mampu menipu *Discriminator*, dan pada akhirnya, menipu persepsi manusia.²

Implikasi dari teknologi ini sangat mendalam. Jika manipulasi tradisional adalah tentang "mengubah" realitas yang sudah ada, *deepfake* adalah tentang "menciptakan" realitas baru. Wajah seseorang dapat ditempelkan ke tubuh orang lain dengan pencahayaan dan ekspresi mikro yang sinkron (*face swap*), atau suara seseorang dapat disintesis untuk mengucapkan kata-kata yang tidak pernah mereka ucapkan (*voice cloning*). Dalam konteks hukum pembuktian, ini meruntuhkan adagium kuno *seeing is believing* (melihat adalah percaya). Hakim Dixon dari Pengadilan Tinggi District of Columbia di Amerika Serikat memperingatkan bahwa fenomena ini dirancang untuk melakukan *gaslighting* terhadap pengamat, menghapus keyakinan dasar bahwa rekaman visual adalah representasi akurat dari peristiwa masa lalu.³

Indonesia tidak kebal terhadap gelombang disrupsi ini. Fenomena *deepfake* telah

¹ Chiquita Thefirstly Noerman and Aji Lukman Ibrahim, "Criminalization of Deepfake in Indonesia as a Form of State Protection," *Jurnal USM Law Review* 7, no. 2 (2024): 603–21.

² Enes Altuncu, Virginia N L Franqueira, and Shujun Li, "Deepfake: Definitions, Performance Metrics and Standards, Datasets, and a Meta-Review," *Front Big Data* 4, no. 7 (2024), <https://doi.org/10.3389/fdata.2024.1400024>.

³ George Bellas, "Deepfakes in the Courtroom: Problems and Solutions," *Illinois State Bar Association* 55, no. 5 (2025), <https://www.isba.org/sections/bench/newsletter/2025/03/deepfakesinthecourtroomproblemsandsolutions>.

bermetamorfosis dari sekadar alat hiburan atau satire menjadi instrumen kejahatan serius (*cybercrime*) yang menyanggar stabilitas politik, integritas finansial, dan martabat individu. Kasus yang paling mencolok dan menjadi *alarm* bagi penegak hukum terjadi pada awal tahun 2025, ketika Direktorat Tindak Pidana Siber Bareskrim Polri mengungkap sindikat penipuan yang menggunakan teknologi *deepfake* untuk mencatut identitas Presiden Prabowo Subianto.⁴ Dalam kasus ini, pelaku tidak sekadar mengedit video lama. Mereka menggunakan AI untuk mensintesis suara (*voice cloning*) dan memanipulasi gerak bibir (*lip-sync*) Presiden, menciptakan video pidato palsu yang menawarkan "bantuan dana syariah" untuk menipu masyarakat. Tingkat sofistikasi serangan ini menunjukkan bahwa *deepfake* telah menjadi alat *social engineering* yang sangat efektif. Korban tidak lagi ditipu oleh teks atau gambar statis, melainkan oleh simulasi audiovisual tokoh otoritas yang mereka percayai. Bareskrim mencatat kerugian materiil, namun kerugian imateriil berupa erosi kepercayaan publik terhadap institusi kepresidenan jauh lebih sulit diukur.⁵

Selain ranah politik dan finansial, sektor yang paling rentan adalah integritas seksual individu. Laporan global dan domestik menunjukkan lonjakan kasus *Non-Consensual Intimate Imagery* (NCII) berbasis *deepfake*. Wajah selebritas Indonesia, tokoh publik, dan bahkan warga biasa, ditempelkan pada tubuh aktor film dewasa.⁶ Fenomena ini diperparah dengan munculnya *AI-generated child sexual abuse material* (AI-CSAM). Meskipun materi ini tidak melibatkan eksploitasi fisik anak secara langsung dalam produksinya, substansinya tetap merupakan kekerasan seksual yang mengganggu ekosistem pedofilia.⁷ Korban dari kejahatan ini sering kali mengalami kesulitan dalam mencari keadilan karena kekosongan definisi hukum: apakah video sintetik yang menampilkan wajah mereka dapat dikategorikan sebagai "pornografi" jika tubuhnya bukan tubuh mereka?

Kasus historis manipulasi video Buni Yani, meskipun terjadi sebelum era *deepfake* canggih, memberikan konteks penting mengenai bagaimana hukum Indonesia merespons modifikasi konten. Dalam kasus tersebut, pengadilan berfokus pada dampak "keonaran" dari penyuntingan manual.⁸ Namun, preseden ini mungkin

⁴ Kurniawan Fadilah, "Pelaku Deepfake Catut Presiden Prabowo Dijerat Pasal Berlapis," *detik.com*, 2025, <https://news.detik.com/berita/d-7768143/pelaku-deepfake-catut-presiden-prabowo-dijerat-pasal-berlapis>.

⁵ Dhika Dwi Putra, "Bareskrim Polri Tegas Berantas Sindikat Deepfake: Bukti Komitmen Penegakan Hukum," *Berita Nasional Update*, 2025, <https://beritanasionalupdate.com/news/details/87/bareskrim-polri-tegas-berantas-sindikat-deepfake:-bukti-komitmen-penegakan-hukum>.

⁶ Komang Bagus Wicaksana Putra and Gusti Ayu Arya Prima Dewi, "Urgensi Pengaturan Tindak Pidana Deepfake Pornografi Di Indonesia," *Jurnal Kertha Wicara* 13, no. 10 (2024): 530–41.

⁷ Putu Nadya Tasya Putri and Anak Agung Ayu Ngurah Tini Rusmini Gorda, "Pengaturan Hukum Dalam Penanggulangan Deepfake Artificial Intelligence (AI) Terhadap Anak Sebagai Korban Kejahatan Siber Di Indonesia," *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* 14, no. 3 (2025): 713–28, <https://doi.org/10.24843/JMHU.2025.v14.i03.p09>.

⁸ ANTARA, "Pengacara Buni Yani Sempat Protes Video JPU," 2017, <https://www.antaraneews.com/berita/642563/pengacara-buni-yani-sempat-protes-video-jpu>.

tidak sepenuhnya relevan atau memadai untuk menghadapi *deepfake* yang dibuat tanpa jejak penyuntingan kasar, yang menimbulkan tantangan baru dalam pembuktian *mens rea* (niat jahat) dan *actus reus* (perbuatan pidana).

Respon hukum Indonesia terhadap ancaman ini cenderung reaktif dan menggunakan instrumen "sapu jagat". Penegak hukum terpaksa melakukan interpretasi ekstensif terhadap pasal-pasal dalam UU ITE (khususnya Pasal 35 tentang manipulasi data dan Pasal 27 tentang kesusilaan) serta KUHP (penipuan dan pencemaran nama baik).⁹ Penerapan pasal-pasal konvensional ini menyisakan celah hukum (*legal loophole*) yang signifikan. Pasal 35 UU ITE, misalnya, mensyaratkan unsur "manipulasi... seolah-olah data yang otentik". Para ahli hukum dan pembela terdakwa dapat berargumen bahwa penciptaan video sintetik dari nol (generatif) bukanlah "manipulasi" terhadap dokumen yang ada, melainkan penciptaan karya fiksi baru. Apakah seorang seniman yang membuat parodi *deepfake* presiden bernyanyi dapat dipidana dengan pasal ini? Tanpa pengecualian yang jelas untuk satir atau karya seni, hukum menjadi tumpul ke atas (sulit menjerat kreator canggih) atau tajam ke samping (mengancam kebebasan berekspresi).¹⁰

Kondisi ini sangat kontras dengan perkembangan global. Tiongkok telah memberlakukan *Deep Synthesis Provisions* yang secara spesifik mengatur kewajiban penyedia layanan untuk melakukan verifikasi identitas (KYC) dan pelabelan konten.¹¹ Uni Eropa melalui *AI Act* Pasal 50 mewajibkan transparansi ketat bagi penyedia sistem AI.¹² Ketidakhadiran regulasi *lex specialis* serupa di Indonesia menempatkan sistem peradilan pada posisi yang rentan, baik dari sisi kemampuan menjerat pelaku maupun kemampuan memvalidasi alat bukti di persidangan.

B. Metode Penelitian

Untuk menyusun artikel yang mendalam, akurat, dan dapat dipertanggungjawabkan secara akademis, penelitian ini menggunakan metodologi penelitian hukum yang ketat. Kompleksitas objek studi yang melintasi batas antara hukum pidana, teknologi informasi, dan hak asasi manusia menuntut penggunaan pendekatan multi-perspektif. Penelitian ini merupakan penelitian hukum normatif (*juridical normative research*). Fokus utama penelitian adalah pada analisis norma hukum tertulis, asas-asas hukum, dan sistematika hukum yang berlaku.¹³ Namun,

⁹ Noerman and Ibrahim, "Criminalization of Deepfake in Indonesia as a Form of State Protection."

¹⁰ Desty Aster Yansen Basah, Andika Wijaya, and Ivans Januardy, "Kriminalisasi Pelanggaran Protokol Digital: Tinjauan Hukum Pidana Terhadap Penyebaran Deepfake Di Media Sosial," *Innovative: Journal Of Social Science Research* 5, no. 4 (2025): 386–398, <https://doi.org/10.31004/innovative.v5i4.20258>.

¹¹ Laney Zhang, "China: Provisions on Deep Synthesis Technology Enter into Effect," *Law Library of Congress*, April 26, 2023, <https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/>.

¹² Natalia Garina, "What the EU's New AI Code of Practice Means for Labeling Deepfakes," *Tech Policy Press*, January 7, 2026, <https://www.techpolicy.press/what-the-eus-new-ai-code-of-practice-means-for-labeling-deepfakes/>.

¹³ Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Prenadamedia Group, 2015).

mengingat sifat teknis dari objek studi (*deepfake*), penelitian ini juga mengintegrasikan elemen *socio-legal* terbatas untuk memahami dampak teknologi terhadap masyarakat dan praktik penegakan hukum.

Untuk membedah permasalahan secara komprehensif, digunakan empat pendekatan utama:

1. Pendekatan Perundang-undangan (*Statute Approach*): Penelitian ini menelaah secara mendalam peraturan perundang-undangan primer di Indonesia (Hierarki Peraturan Perundang-undangan) untuk menginventarisasi dan menganalisis pasal-pasal yang relevan.
2. Pendekatan Konseptual (*Conceptual Approach*): Penelitian ini merujuk pada doktrin hukum dan pandangan ahli untuk mendefinisikan konsep-konsep baru yang belum memiliki definisi legal yang mapan. Konsep "Kebenaran Sintetik", "Manipulasi Generatif", dan "Identitas Biometrik Digital" dianalisis untuk menguji relevansi terminologi hukum saat ini ("Informasi Elektronik", "Dokumen Elektronik").
3. Pendekatan Perbandingan (*Comparative Approach*): Penelitian ini melakukan perbandingan hukum (*legal comparison*) dengan yurisdiksi asing yang telah memiliki regulasi maju terkait AI, untuk menemukan best practices dan mengukur keteringgalan Indonesia.
4. Pendekatan Kasus (*Case Approach*): Meskipun yurisprudensi *deepfake* murni masih jarang, penelitian ini menganalisis putusan dan kasus terkait manipulasi elektronik yang menjadi embrio.

Selanjutnya bahan hukum yang terkumpul dianalisis secara kualitatif dengan metode silogisme deduktif. Premis mayor (aturan hukum) dipertemukan dengan premis minor (fakta teknologi *deepfake*) untuk menarik kesimpulan mengenai ada atau tidaknya kekosongan hukum dan bagaimana dampaknya terhadap sistem pembuktian.

C. Pembahasan

1. Problematika Kekosongan Norma Hukum Materiel dalam Menjerat Pelaku *Deepfake*

Bagian ini menyajikan analisis mendalam mengenai kerangka hukum materiel (*substantive law*) di Indonesia. Fokus utama adalah membuktikan hipotesis bahwa instrumen hukum yang ada saat ini mengandung kekosongan norma (*legal vacuum*) yang signifikan ketika berhadapan dengan sifat ontologis teknologi *deepfake*. Pasal 35 UU ITE sering dianggap sebagai *panacea* (obat segala penyakit) untuk kejahatan siber yang melibatkan rekayasa data. Pasal ini 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."

Secara sekilas, pencantuman kata "penciptaan" (*creation*) dan "manipulasi" tampaknya cukup untuk menjerat pembuat *deepfake*. Namun, analisis dogmatik yang lebih dalam mengungkap kelemahan fundamental:

- a. Ambiguitas Konsep "Otentik": Inti dari delik Pasal 35 adalah penipuan terhadap otentisitas (*authenticity*). Dalam konteks konvensional, "palsu" berarti tidak sesuai dengan aslinya (misalnya, scan KTP yang tanggal lahirnya diubah). Namun, *deepfake* bekerja dengan cara yang berbeda:
 - 1) AI tidak sekadar "mengubah" video A. AI mempelajari pola wajah A, lalu *menciptakan* piksel-piksel baru yang membentuk wajah A pada posisi yang ditentukan.
 - 2) Hasil akhirnya adalah sebuah *file* video baru yang secara teknis (metadata) adalah "asli" buatan komputer, bukan hasil *editing* dari file kamera.
 - 3) Pertanyaan hukumnya: Jika sebuah video *deepfake* dibuat dari nol (sintetis), apakah ia "seolah-olah data yang otentik"? Jika kreatornya berargumen bahwa video tersebut adalah "karya seni digital" atau "simulasi", unsur penipuan terhadap otentisitas menjadi kabur. Berbeda dengan pemalsuan surat yang memiliki pembanding asli, video *deepfake* pidato presiden yang *tidak pernah terjadi* tidak memiliki pembanding asli untuk membuktikan kepalsuannya secara langsung.¹⁴
- b. Ketiadaan Pengecualian untuk Satir dan Seni: Pasal 35 tidak memiliki klausul pengecualian (*defense*) untuk parodi atau satir. Hal ini berbahaya. Seorang kreator konten yang membuat video *deepfake* pejabat bernyanyi lagu dangdut untuk tujuan kritik sosial atau humor bisa saja dijerat dengan pasal ini karena telah "menciptakan informasi seolah-olah otentik". Ketiadaan batasan yang jelas antara malicious *deepfake* (jahat) dan creative *deepfake* (seni) menciptakan ketidakpastian hukum yang dapat memberangus kebebasan berekspresi, atau sebaliknya, digunakan oleh pelaku kejahatan untuk berlindung di balik dalih "ini hanya parodi".¹⁵
- c. Masalah Kausalitas Kerugian (Delik Formil vs Materiil): Meskipun Pasal 35 dikonstruksikan sebagai delik formil, penegakan hukum sering mengaitkannya dengan kerugian (Pasal 51). Untuk *deepfake* yang bertujuan disinformasi politik (seperti kasus Prabowo), kerugiannya adalah "gangguan ketertiban umum" atau "erosi kepercayaan". Pembuktian hubungan kausalitas antara video *deepfake* dan kerugian abstrak ini sering kali rumit di pengadilan, berbeda

¹⁴ Basah, Wijaya, and Januardy, "Kriminalisasi Pelanggaran Protokol Digital: Tinjauan Hukum Pidana Terhadap Penyebaran Deepfake Di Media Sosial."

¹⁵ Siti Nurkholisah et al., "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia," *Jurnal USM Law Review* 8, no. 3 (2025): 2421–45, <https://doi.org/10.26623/julr.v8i3.13060>.

dengan penipuan transfer uang yang jejak kerugiannya jelas.¹⁶

2. KUHP Baru dan Keterbatasan Paradigma Penipuan Konvensional

Berlakunya KUHP Baru (UU No. 1 Tahun 2023) mulai Januari 2026 diharapkan membawa pembaruan. Pasal 492 KUHP Baru mengatur tentang tindak pidana penipuan melalui alat elektronik.

- a. Teks Pasal: Mengancam pidana bagi setiap orang yang melakukan tipu muslihat atau rangkaian kebohongan melalui sistem elektronik yang mengakibatkan kerugian materiil bagi orang lain.¹⁷
- b. Analisis Kesenjangan: Pasal ini masih sangat berorientasi pada kerugian *materiil* (harta benda). Bagaimana dengan *deepfake* yang merusak reputasi atau menyebabkan trauma psikologis tanpa kerugian finansial langsung? Sebagai contoh dalam kasus pornografi *deepfake* (NCII) sering kali tidak melibatkan pemerasan uang. Motifnya bisa balas dendam atau kepuasan seksual semata. Dalam skenario ini, Pasal 492 KUHP Baru menjadi tidak relevan. Penegak hukum terpaksa kembali ke pasal pencemaran nama baik (Pasal 433 KUHP Baru) atau pornografi, yang masing-masing memiliki kelemahan tersendiri.¹⁸

Salah satu kekosongan hukum yang paling mencolok dan berbahaya adalah dalam penanganan *Deepfake Pornography*. UU Pornografi (No. 44 Tahun 2008) mendefinisikan pornografi sebagai gambar, sketsa, foto, dll., yang memuat kecabulan. Sementara dalam video *deepfake* porno, tubuh yang melakukan adegan seks biasanya adalah aktor profesional (legal di negara asalnya), sedangkan wajahnya adalah wajah korban (tempelan). Secara teknis, korban *tidak pernah* melakukan adegan tersebut. Oleh karena itu, pelaku bisa berargumen: "Saya tidak merekam korban telanjang. Saya hanya membuat animasi wajah." Dalam hukum Indonesia belum secara eksplisit mengakui "Identitas Biometrik Virtual" sebagai objek yang harus dilindungi setara dengan tubuh fisik. Akibatnya, pelaku sering kali hanya dikenakan pasal penyebaran konten asusila (UU ITE Pasal 27), yang ancaman hukumannya mungkin tidak sebanding dengan dampak seumur hidup bagi korban.¹⁹

Kekosongan ini semakin parah pada kasus *AI-CSAM* (Pornografi Anak AI). Karena tidak ada anak "nyata" yang disakiti dalam pembuatan videonya (karena anak tersebut adalah hasil generasi komputer), pelaku dapat lolos dari jeratan

¹⁶ Putra, "Bareskrim Polri Tegas Berantas Sindikat Deepfake: Bukti Komitmen Penegakan Hukum."

¹⁷ SIP Law Firm, "Pidana Atas Konten Deepfake, Tantangan Baru Penegakan Hukum Di Era AI," 2025, <https://siplawfirm.id/konten-deepfake/?lang=id>.

¹⁸ Putra and Dewi, "Urgensi Pengaturan Tindak Pidana Deepfake Pornografi Di Indonesia."

¹⁹ Putra and Dewi.

pasal perlindungan anak yang mensyaratkan adanya korban anak fisik.²⁰ Untuk memvalidasi argumen kekosongan hukum ini, perbandingan dengan kerangka hukum di Tiongkok dan Uni Eropa menunjukkan betapa jauhnya kesenjangan regulasi yang ada.

Tabel 1. Perbandingan Kerangka Hukum Deepfake: Indonesia, Tiongkok, dan Uni Eropa

Aspek Regulasi	Indonesia (Status Quo)	Tiongkok (Deep Synthesis Provisions 2023)	Uni Eropa (EU AI Act 2024)
Definisi Legal	Tidak ada. Mengindik pada definisi umum "Informasi Elektronik" dan "Dokumen Elektronik".	Ada (<i>Deep Synthesis Technology</i>). Didefinisikan rinci mencakup <i>text-to-speech, face swap, gesture manipulation</i> , VR, dll.	Ada (<i>Deep Fake</i>). Didefinisikan sebagai konten manipulasi/sintetik yang secara salah tampak otentik atau jujur.
Kewajiban Labeling (<i>Watermarking</i>)	Tidak Ada. Tidak ada kewajiban hukum bagi kreator/platform untuk memberi tanda pada konten AI.	Wajib & Ketat. Penyedia layanan <i>harus</i> memberi label " <i>Synthetic</i> " yang jelas pada output. Konten tanpa label ilegal.	Wajib (<i>Transparency Obligation</i> - Art 50). Penyedia sistem dan pengguna (<i>deployer</i>) wajib mengungkapkan asal usul konten sintetik kepada audiens.
Persetujuan Subjek (<i>Consent</i>)	Umum (UU PDP). Persetujuan pemrosesan data pribadi secara umum.	Spesifik & Wajib. Mengedit biometrik (wajah/suara) orang lain memerlukan persetujuan eksplisit dari individu tersebut.	Diatur ketat di bawah GDPR dan diperkuat AI Act untuk sistem berisiko tinggi (<i>High Risk AI</i>).
Tanggung Jawab Platform	<i>Safe Harbor</i> pasif. Bertindak <i>notice-and-takedown</i> (menunggu laporan).	Tanggung Jawab Aktif. Platform wajib memoderasi konten, memverifikasi identitas asli pengguna (<i>Real-</i>	Fokus pada akuntabilitas Penyedia (<i>Provider</i>) dan Pengguna (<i>Deployer</i>). Sanksi

²⁰ Putri and Gorda, "Pengaturan Hukum Dalam Penanggulangan Deepfake Artificial Intelligence (AI) Terhadap Anak Sebagai Korban Kejahatan Siber Di Indonesia."

		<i>name registration</i>), dan mendeteksi deepfake.	denda administratif sangat besar.
Pendekatan Hukum	Represif (<i>Ex-Post</i>). Menindak setelah kejadian/viral/ada kerugian.	Preventif & Administratif (<i>Ex-Ante</i>). Mencegah peredaran melalui kontrol algoritma dan registrasi.	Berbasis Risiko (<i>Risk-Based</i>). Tingkat regulasi tergantung tingkat risiko aplikasi AI.

Tabel di atas mengilustrasikan bahwa Indonesia masih berada pada tahap *ex-post enforcement*, hanya bereaksi setelah kejahatan terjadi. Sebaliknya, Tiongkok dan UE telah menerapkan *ex-ante regulation*, yakni pencegahan melalui kewajiban transparansi teknologi. Kekosongan regulasi preventif di Indonesia (seperti ketiadaan wajib *watermarking*) membuat pembuktian di pengadilan menjadi sangat sulit karena tidak adanya jejak asal-usul (*provenance*) pada file video.²¹

3. Ancaman Pembuktian Hukum Acara dan Integritas Peradilan

Salah satu ancaman terbesar yang ditimbulkan oleh *deepfake* terhadap sistem peradilan dikenal sebagai *The Deepfake Defense* atau "Pembelaan Deepfake". Fenomena ini berkaitan erat dengan konsep *Liar's Dividend* (Dividen Pembohong). Keberadaan teknologi *deepfake* yang diketahui umum menciptakan skeptisisme universal terhadap bukti video. Pelaku kejahatan yang *benar-benar* terekam melakukan kejahatan (misalnya, terekam CCTV menerima suap atau melakukan kekerasan) dapat dengan mudah menyangkal bukti tersebut di pengadilan dengan klaim: "Itu bukan saya, Yang Mulia. Itu adalah video *deepfake* yang dibuat oleh musuh politik saya untuk menjebak saya."²²

Dalam hukum acara pidana Indonesia, hakim harus memutus berdasarkan "sekurang-kurangnya dua alat bukti yang sah" dan keyakinan hakim (Pasal 183 KUHP). Jika terdakwa berhasil menanamkan *Reasonable Doubt* (keraguan yang beralasan) bahwa video tersebut *mungkin* palsu, hakim yang berpegang pada prinsip *in dubio pro reo* (jika ragu, putuslah yang meringankan terdakwa) mungkin akan mengesampingkan bukti video tersebut. Akibatnya, bukti video yang selama ini dianggap sebagai "Golden Evidence" (bukti emas) kehilangan kekuatannya. Jaksa Penuntut Umum (JPU) kini memikul beban pembuktian yang jauh lebih berat: tidak hanya membuktikan isi video, tetapi juga membuktikan secara forensik bahwa video tersebut *bukan* hasil rekayasa AI. Ini adalah beban yang sangat berat

²¹ Linklaters LLP, "Regulating ChatGPT and the Metaverse for Social Good: How Do China's First-Ever Deepfake Rules Affect AI Governance," 2023, <https://techinsights.linklaters.com/post/102iitc/regulating-chatgpt-and-the-metaverse-for-social-good-how-do-chinas-first-ever-d>.

²² Bellas, "Deepfakes in the Courtroom: Problems and Solutions."

dan mahal.²³

Pasal 5 ayat (1) UU ITE menyatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik adalah alat bukti hukum yang sah. Namun, Pasal 6 menetapkan syarat agar dianggap sah, yakni harus dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan. Lalu pertanyaannya adalah bagaimana cara mempertanggungjawabkan video *deepfake* yang dibuat oleh akun anonim menggunakan server di luar negeri? Video *deepfake* yang menyebar di WhatsApp mengalami kompresi berulang kali. Kompresi ini merusak struktur metadata dan *hash* file. Ketika ahli forensik memeriksa file tersebut, mereka mungkin menemukan bahwa integritas file sudah "rusak" (tidak identik dengan master file asli). Dalam paradigma forensik konvensional, file yang rusak integritasnya lemah nilai pembuktiannya. Ironisnya, hal ini justru menguntungkan pembuat *deepfake*: jejak manipulasi AI (artefak) hilang tertutup oleh artefak kompresi, membuat deteksi menjadi mustahil.

Kesiapan infrastruktur forensik digital di Indonesia menghadapi tantangan berat. Hubungan antara pembuat *deepfake* (*Generator*) dan pendeteksi (*Detector*) adalah sebuah perlombaan senjata yang tak berujung.

- a. Keterbatasan Teknis Laboratorium: Bareskrim Polri memiliki laboratorium siber yang canggih, terbukti dalam pengungkapan kasus *deepfake* Prabowo.²⁴ Namun, kapasitas ini belum merata hingga ke tingkat Polda atau Polres. Kasus-kasus di daerah mungkin tidak mendapatkan penanganan forensik dengan standar yang sama. Keterbatasan tools deteksi AI yang mahal dan membutuhkan daya komputasi tinggi (GPU Cluster) menjadi hambatan logistik.
- b. Ketiadaan Standar Deteksi Nasional (SNI): Indonesia telah mengadopsi SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Koleksi, Akuisisi, dan Preservasi Bukti Digital.²⁵ Namun, standar ini lebih berfokus pada *Chain of Custody* fisik (bagaimana menyita *hard disk* agar data tidak berubah). Oleh karena itu, belum ada SNI khusus yang mengatur Metodologi Analisis Deteksi Deepfake. Apakah deteksi harus menggunakan analisis *Biological Signals* (detak jantung visual)? Analisis *Frequency Domain*? Atau analisis *Consistency of Lighting*? Dengan demikian, tanpa standar baku, hasil pemeriksaan ahli forensik di pengadilan menjadi rentan didebat (*debatable*). Ahli dari pihak terdakwa dapat menggunakan metode yang berbeda untuk menghasilkan kesimpulan yang berlawanan ("Video ini asli" vs "Video ini palsu"), yang pada

²³ Anandy Satrio P, "Deepfake Dilema: Tantangan Hukum Pidana Di Era Artificial Intelligence," Dandapala Contributor, 2025, <https://www.dandapala.com/opini/detail/deepfake-dilema-tantangan-hukum-pidana-di-era-artificial-intelligence>.

²⁴ Fadilah, "Pelaku Deepfake Catut Presiden Prabowo Dijerat Pasal Berlapis."

²⁵ adminwqa, "ISO 27037 Untuk Digital Forensik," WQA INDONESIA, 2025, <https://wqa.co.id/iso-27037-untuk-digital-forensik/>.

akhirnya membingungkan hakim dan mengaburkan kebenaran materiil.²⁶

- c. Masalah *Chain of Custody* (Rantai Pasok Bukti) Non-Fisik: SOP Forensik Polri dan Kejaksaan (Peraturan Jaksa Agung No. 7 Tahun 2020) sangat ketat soal barang bukti fisik. Namun, *deepfake* sering kali eksis di cloud atau media sosial. Penyitaan "url" atau "screenshot" tidak cukup untuk membuktikan asal-usul algoritma. Penegak hukum perlu kemampuan untuk melakukan *traceback* ke sumber uploader pertama, yang sering kali terhalang oleh enkripsi platform dan yurisdiksi lintas negara.

Dalam studi kasus seperti Putusan Buni Yani (Putusan MA yang menguatkan vonis PN Bandung), justru memberikan wawasan tentang bagaimana hakim memandang "pengubahan" bukti elektronik.²⁷ Buni Yani divonis bukan karena membuat video palsu, tetapi karena memotong durasi dan menambahkan *caption* yang provokatif, yang dianggap "mengubah" informasi elektronik sehingga menimbulkan rasa kebencian (Pasal 28 ayat 2 UU ITE).

Putusan ini menegaskan bahwa "modifikasi" yang mengubah makna/konteks dapat dipidana. Ini menjadi dasar hukum (yurisprudensi) untuk menjerat penyebar *deepfake* yang memodifikasi konteks kebenaran. Namun terdapat sisi negatif (tantangan) dalam kasus Buni Yani yang melibatkan video *asli* yang dipotong. Ada video "Master" (asli) sebagai pembanding. Dalam kasus *deepfake* generatif, sering kali tidak ada video master. Video tersebut diciptakan dari ketiadaan. Tanpa pembanding, bagaimana hakim bisa yakin 100% bahwa itu adalah modifikasi dan bukan kejadian asli (jika sangat sempurna)? Di sinilah letak bahaya *Deepfake Defense* yang belum terjawab oleh preseden Buni Yani.

D. Kesimpulan

Terjadi Kekosongan Norma Hukum Materiel (*Substantive Legal Vacuum*), bahwa hukum pidana Indonesia (UU ITE, KUHP, UU PDP) saat ini bersifat gagap teknologi dalam menghadapi *deepfake*. Definisi "manipulasi" dalam Pasal 35 UU ITE terlalu sempit dan ambigu untuk menjangkau sifat "generatif" AI. Tidak adanya kategori hukum untuk "Kebenaran Sintetik" dan ketiadaan kewajiban transparansi (*watermarking*) seperti di Tiongkok dan UE menciptakan ekosistem di mana disinformasi dapat berkembang biak tanpa hambatan regulasi preventif. Perlindungan terhadap korban NCII juga sangat lemah karena ketiadaan pengakuan terhadap hak atas identitas biometrik virtual. Oleh karena itu terdapat ancaman nyata terhadap integritas pembuktian (*evidentiary threat*), bahwa teknologi *deepfake* telah memicu krisis epistemologis di ruang sidang. Fenomena "*Deepfake Defense*" mengancam untuk mendevaluasi alat bukti video, mempersulit tugas Jaksa Penuntut

²⁶ Herman et al., "Use of Digital Forensics in Proving the Criminal Offense of Damage to Good Name in Social Media Based on the Law of Information and Electronic Transactions," *Halu Oleo Legal Research* 6, no. 2 (2024): 588–603.

²⁷ ANTARA, "Pengacara Buni Yani Sempat Protes Video JPU."

Umum, dan meningkatkan biaya penegakan hukum akibat kebutuhan forensik tingkat tinggi. Ketiadaan standar nasional deteksi *deepfake* dan keterbatasan kapasitas forensik di daerah memperburuk risiko *miscarriage of justice*.

Referensi

- adminwqa. "ISO 27037 Untuk Digital Forensik." WQA INDONESIA, 2025. <https://wqa.co.id/iso-27037-untuk-digital-forensik/>.
- Altuncu, Enes, Virginia N L Franqueira, and Shujun Li. "Deepfake: Definitions, Performance Metrics and Standards, Datasets, and a Meta-Review." *Front Big Data* 4, no. 7 (2024). <https://doi.org/10.3389/fdata.2024.1400024>.
- ANTARA. "Pengacara Buni Yani Sempat Protes Video JPU," 2017. <https://www.antaranews.com/berita/642563/pengacara-buni-yani-sempat-protes-video-jpu>.
- Basah, Desty Aster Yansen, Andika Wijaya, and Ivans Januardy. "Kriminalisasi Pelanggaran Protokol Digital: Tinjauan Hukum Pidana Terhadap Penyebaran Deepfake Di Media Sosial." *Innovative: Journal Of Social Science Research* 5, no. 4 (2025): 386–398. <https://doi.org/10.31004/innovative.v5i4.20258>.
- Bellas, George. "Deepfakes in the Courtroom: Problems and Solutions." *Illinois State Bar Association* 55, no. 5 (2025). <https://www.isba.org/sections/bench/newsletter/2025/03/deepfakesinthecourtroomproblemsandsolutions>.
- Fadilah, Kurniawan. "Pelaku Deepfake Catut Presiden Prabowo Dijerat Pasal Berlapis." *detik.com*, 2025. <https://news.detik.com/berita/d-7768143/pelaku-deepfake-catut-presiden-prabowo-dijerat-pasal-berlapis>.
- Garina, Natalia. "What the EU's New AI Code of Practice Means for Labeling Deepfakes." *Tech Policy Press*, January 7, 2026. <https://www.techpolicy.press/what-the-eus-new-ai-code-of-practice-means-for-labeling-deepfakes/>.
- Herman, Handrawan, Oheo Kaimuddin Haris, Sitti Aisah Abdullah, Ali Rizky, and Sri Ratih Indah. "Use of Digital Forensics in Proofing the Criminal Offense of Damage to Good Name in Social Media Based on the Law of Information and Electronic Transactions." *Halu Oleo Legal Research* 6, no. 2 (2024): 588–603.
- Linklaters LLP. "Regulating ChatGPT and the Metaverse for Social Good: How Do China's First-Ever Deepfake Rules Affect AI Governance," 2023. <https://techinsights.linklaters.com/post/102iitc/regulating-chatgpt-and-the-metaverse-for-social-good-how-do-chinas-first-ever-d>.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Prenadamedia Group, 2015.
- Noerman, Chiquita Thefirstly, and Aji Lukman Ibrahim. "Criminalization of Deepfake in Indonesia as a Form of State Protection." *Jurnal USM Law Review* 7, no. 2 (2024): 603–21.

- Nurkholisah, Siti, Daud Rismansa, Afrizal Eko Nugroho, Amrina Munjiyah, and Qurota Ayunisa. "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia." *Jurnal USM Law Review* 8, no. 3 (2025): 2421–45. <https://doi.org/10.26623/julr.v8i3.13060>.
- P, Anandy Satrio. "Deepfake Dilema: Tantangan Hukum Pidana Di Era Artificial Intelligence." Dandapala Contributor, 2025. <https://www.dandapala.com/opini/detail/deepfake-dilema-tantangan-hukum-pidana-di-era-artificial-intelligence>.
- Putra, Dhika Dwi. "Bareskrim Polri Tegas Berantas Sindikat Deepfake: Bukti Komitmen Penegakan Hukum." Berita Nasional Update, 2025. <https://beritanasionalupdate.com/news/details/87/bareskrim-polri-tegas-berantas-sindikat-deepfake:-bukti-komitmen-penegakan-hukum>.
- Putra, Komang Bagus Wicaksana, and Gusti Ayu Arya Prima Dewi. "Urgensi Pengaturan Tindak Pidana Deepfake Pornografi Di Indonesia." *Jurnal Kertha Wicara* 13, no. 10 (2024): 530–41.
- Putri, Putu Nadya Tasya, and Anak Agung Ayu Ngurah Tini Rusmini Gorda. "Pengaturan Hukum Dalam Penanggulangan Deepfake Artificial Intelligence (AI) Terhadap Anak Sebagai Korban Kejahatan Siber Di Indonesia." *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* 14, no. 3 (2025): 713–28. <https://doi.org/10.24843/JMHU.2025.v14.i03.p09>.
- SIP Law Firm. "Pidana Atas Konten Deepfake, Tantangan Baru Penegakan Hukum Di Era AI," 2025. <https://siplawfirm.id/konten-deepfake/?lang=id>.
- Zhang, Laney. "China: Provisions on Deep Synthesis Technology Enter into Effect." *Law Library of Congress*, April 26, 2023. <https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/>.