KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Penelitian Mahasiswa (JIPM)
Vol.4, No.6 Desember 2026
e-ISSN: 3025-5465, p-ISSN : 3025-7964, Hal 1335-1350
DOI : https://doi.org/10.61722/jipm.v4i6.3298

Penegakan Hukum terhadap Penipuan Deepfake AI di Indonesia: Analisis Yuridis Kasus Polda Jawa Timur dan Rekomendasi Reformulasi Regulasi

Nabila Maylina Putri Ardineatha[1] , Revita Indri Kusumawardani[2] , Salsabila Ardhia Izza Alfathi[3] , Artamevia Berline Arsetya[4]
[1-4] Prodi Ilmu Hukum, Fakultas Hukum dan Ilmu Politik
Universitas Muhammadiyah Surakarta
*Penulis Korespondensi: c100240177@student.ums.ac.id, c100240180@student.ums.ac.id, c100240185@student.ums.ac.id, c100240188@student.ums.ac.id

Abstract. *The development of generative artifical intelligence has given rise to a new form of crime: deepfake-based fraud, which causes losses to the public. One such case was uncovered by Cyber Crime Directorate of the East Java Regional Police in April 2025. Three suspects used deepfake technology to alter the face and voice of the Governor of East Java in order to promise cash assistance, and obtained approximately IDR 87.6 million from victims in four provinces. The article examines how Indonesian positive law, particularly Law Number 1 of 2024 on the Second Amendment to the Electronic Information and Transactions (EIT) Law and Law Number 1 of 2023 on the Criminal Code, covers the criminal act of deepfake fraud. It also identifities challenges in law enforcement and offers recommendations of optimizing perfomance. This study employs a normative juridical method with statutory and case approaches, and the results are analyzed qualitatively through content analysis. The findings show that: (1) general provisions of the EIT Law, such as Article 35 in conjunction with Article 51 paragraph (1) and Article 45A paragraph (1), can still be used to prosecute offenders, but there is no specific regulation or definiton of deepfakes, resulting in a legal vacuum; (2) legal obstacles include the absence of an official definition and difficulties in proving cases digitally, while non-legal obstacles include investigators' limited capacity to trace digital evidence, the public' low understanding of digital technology, insufficient cooperation from digital platform owners, and weak coordination among agencies; and (3) to improve law enforcement, it is necessary to revise regulatioms gradually (implementing regulations, amendments to the EIT Law, and eventually a dedicated law on artifical intelliegence), strengthen the capacity of law enforcement officers, including digital forensic laboratories, enhance collaboration among stakeholders, and increase public understanding of digital technology.*

Keywords: *Deepfake, Fraud, Law Enforcement, EIT Law, Artifical Intelligence*

Abstrak. Perkembangan teknologi kecerdasan buatan generatif menciptakan modus kejahatan baru berupa penipuan berbasis deepfake, yang mengakibatkan kerugian bagi masyarakat. Salah satu kasusnya diungkap oleh Direktorat Reserse Siber Polda Jawa Timur pada April 2025. Tiga tersangka mengubah wajah dan suara Gubernur Jawa Timur menggunakan teknologi deepfake untuk menjanjikan bantuan uang, dan berhasil memperoleh keuntungan sekitar Rp. 87,6 juta dari korban di empat provinsi. Artikel ini membahas bagaimana hukum positif di Indonesia, terutama Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua Undang-Undang ITE dan Undang-Undang Nomor 1 Tahun 2023 tentang KUHP, mencakupi tindak pidana penipuan deepfake. Artikel ini juga menemukan tantangan dalam penerapan hukum dan memberikan saran untuk meningkatkan kinerja secara optimal. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan serta pendekatan kasus, dan hasilnya dianalisis secara kualitatif dengan cara analisis isi. Hasil penelitian menunjukkan bahwa: (1) pasal-pasal umum UU ITE, seperti Pasal 35 jo. Pasal 51 ayat (1) dan Pasal 45A ayat (1) masih bisa digunakan untuk menangani pelaku, tetapi belum ada aturan atau definisi khusus mengenai deepfake, sehingga terjadi kekosongan dalam aturan hukum; (2) hambatan dalam hukum meliputi tidak adanya definisi resmi dan kesulitan dalam membuktikan kasus secara digital, sedangkan hambatan non-hukum mencakup keterbatasan kemampuan penyidik dalam menelusuri bukti digital, rendahnya pemahaman masyarakat mengenai teknologi digital, kurangnya kerjasama dari pemilik platform digital, serta kurangnya kerja sama antar instansi; dan (3) untuk meningkatkan penerapan hukum, perlu adanya revisi peraturan secara bertahap (aturan turunan, perubahan

Naskah Masuk: 25 Oktober 2026; Revisi: 26 Oktober 2026; Diterima: 27 Oktober 2026; Terbit: 31 Oktober 2026

UU ITE, hingga undang-undang khusus mengenai kecerdasan buatan), peningkatan kemampuan aparatur termasuk laboraturium forensik digital, kolaborasi antar pihak, serta peningkatan pemahaman masyarakat tentang teknologi digital.

Kata kunci: *deepfake,* Penipuan, Penegakan Hukum, UU ITE, Kecerdasan buatan

1. LATAR BELAKANG

Era revolusi industri 4.0 telah membawa transformasi mendasar dalam kehidupan Masyarakat, termasuk dalam dimensi kejahatan. Teknologi kecerdasan buatan (artificial intelligence/ AI) yang semula dikembangkan untuk tujuan produktif, kini disalahgunakan sebagai alat kejahatan yang modern. dengan penyalahgunaan dari media yang semakin canggih dan sulit dideteksi. Salah satu manifestasi paling menghawatirkan Adalah teknologi deepfake, yakni Teknik manipulasi digital berbasis AI yang mampu menciptakan video, gambar, atau suara palsu yang tampak nyata dan meyakinkan.

Bangsa Indonesia tidak luput dari ancaman ini, berdasarkan laoran Liputan 6 (2024), modus penipuan deepfake di Indonesia meningkat drastic hingga 1.550 persen dalam satu tahun terakhir. Deepfake telah menjadi ancaman serius dalam kejahatan siber, memungkinkan pelaku untuk menipu Masyarakat dengan manipulasi video dan audio yang sangat realistis.[1] Tren ini mencapai puncaknya puncaknya Ketika Direktorat Reserse Siber Polda Jawa Timur menggelar konferensi pers pada tanggal 28 April 2025 untuk mengungkap kasus penipuan berbasis deepfake yang menggunakan wajah dan suara Gubernur Jawa Timur, Khofifah Indar Parawansa. Tiga tersangka , yakni HMP (32),UP (24), dan AH (34), semuanya warga Kabupaten Pangandaran, Jawa Barat, berhasil meraup keuntungan sebesar Rp 87.600.000 selama tiga bulan beroparasi, dengan korban tersebar di empat provinsi.

Kasus ini menjadi tolok ukur penting bagi system hukum Indonesia dalam menghadapi kejahatan berbasis AI. Di satu sisi, pemgungkapan kasus ini membuktikan bahwa aparat penegak hukum mampu mendeteksi dan menidak kejahatan siber modern. Disisi lain, kasus ini juga mengekspos kelemahan regulasi yang ada, karena Indonesia

[1] Yoan Shevila Kristiyenda, Jasmine Faradila, and Christina Basanova, "Pencegahan Kejahatan Deepfake: Studi Kasus Terhadap Modus Penipuan Deepfake Prabowo Subianto Dalam Tawaran Bantuan Uang," *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (2025): 149–64, https://doi.org/10.59246/aladalah.v3i2.1263.

hingga saat ini belum memiliki undang-undang khusus yang mengatur deepfake sebagai tindak pidana tersendiri. Secara teknis, hambatan utama dalam penegakan hukum terhadap deepfake Adalah keterbatasan teknologi forensic dan sumber daya manusia. Sebagaimana dilaporkan oleh BSSN hanya 15% penegak hukum Indonesia memiliki pelatihan forensic digital yang memadai untuk mendeteksi deepfake pada tahun 2025, dengan jumlah yang lebih rendah di wilayah terpeci seperti Maluku dan Papua.[2]

Kondisi ini menimbulkan pertanyaan akademis yang krusial: bagaimana hukum positif Indonesia menjangkau kejahatan deepfake, apa hambatan yang dihadapi, dan bagaimana optimalisasi penegakan hukum dapat dilakukan secara sistematik? Pertanyaan-pertanyaan ini menjadi pokok bahasan dalam artikel ilmiah ini.

2. METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normative (normative legal research), yaitu penelitian yaitu penelitian yang mengkaji hukum berdasarkan bahan-bahan hukum yang ada, baik hukum yang tertulis maupun yang tidak tertulis, serta prinsip-prinsip hukum yang berlaku. Khususnya dalam menganalisis adanya kekosongan hukum (legal vacuum) terkait penanganan deepfake sebagai alat kejahatan siber.

1) Pendekatan Penelitian

Penelitian ini menggunakan dua pendekatan secara komplementer;

- Pendekatan perundang-undangan (statue Appoarch): mengkaji seluruh regulasi yang relevan dengan kejahatan deepfake di Indonesia. Yakni UU No 1 Tahun 2024 tentang ITE, UU No 1 Tahun 2023 tentang KUHP serta regulasi turunnya.
- Pendekatan kasus (Case Appoarch): menganalisi kasus penipuan deepfake yang diungkap Polda Jatim pada April 2025 sebagai bahan studi kasus utama, meliputi modus operandi, konstruksi dakwaan, dan implikasi hukumnya.

2) Sumber dan Bahan Hukum

[2] Siti Nurkholisah et al., "Tantangan Kriminalisasi Deepfake Dalam Hukum Pidana Indonesia Challenges in Criminalizing Deepfakes under Indonesian Criminal Law," *Jurnal Usm Law Review* 8, no. 3 (2025): 1–12, https://journals.usm.ac.id/index.php/julr/article/view/13060.

- Bahan hukum primer: UU No 1 Tahun 2024 tentang perubahan kedua UU ITE, UU No 1 Tahun 2023 tentang KUHP, Putusan Mahkamah Konstitusi, serta dokumen resmi Polda Jatim terkait kasus.
- Bahan hukum sekunder: literatur ilmiah, jurnal hukum, artikel akademis, berita resmi, dan laporan instansi pemerintah
- Bahan hukum tersier: kamus hukum, enslikopedia, serta sumber referensi digital yang relevan.

C. Metode Analisis Data

Data yang telah dikumpulkan dianalisis dengan metode kualitatif menggunakan Teknik analisis isi. Dalam proses analisis, beberapa tahap dilakukan, antara lain identifikasi peraturan yang mengatur tentang kasus deepfake sebelum dan sesudah perubahan. Klasifikasi data hukum berdasarkan sumbernya (primer dan sekunder). Interpretasi makna tentang Optimalisasi penegakan hukum terhadap penipuan Deepfake AI berdasarkan teori hukum dan doktrin hukum yang relevan. Serta penyusunan Kesimpulan terkait dampak deepfake dan implikasi hukum nya dalam system hukum nasional.

Metode penelitian ini diharapkan dapat memberikan analisis yang komprehensif mengenai penegakan hukum terhadap penipuan deepfake AI dalam UU No 1 Tahun 2024 tentang perubahan UU ITE kedua serta implikasinya terhadap system hukum di Indonesia.

3. HASIL DAN PEMBAHASAN

1. Konstruksi hukum positif Indonesia dalam menjangkau kejahatan penipuan berbasis teknologi deepfake AI

Perkembangan deepfake di Indonesia mulai menarik perhatian publik karena banyaknya kasus penyebaran konten manipulative yang mencoreng reputasi seseorang atau bahkan membawa meraka ke Tindakan criminal. Jumlah konten deepfake yang tersebar di berbagai platform internet, terutama media social telah meningkat sebagai akibat dari kemudahan mendapat teknologi ini. Dari perspektif hukum pidana,

penyebaran konten deepfake melibatkan elemen pemalsuan, penipuan pencemaran nama baik, dan pelanggaran hak privasi seseorang.[3]

Dalam UU perlindungan saksi dan korban (LPSK), pasal 1 mendefinisikan korban sebagai seseorang yang mengalami penderitaan fisik, mental, atau ekonomi yang disebabkan oleh tindak pidana, dalam pasal 3 dijelaskan bahwa LPSK Adalah Lembaga yang bertanggung jawab untuk memberikan perlindungan dan hak-hak lain kepada saksi dam atau korban tindak pidana.[4]

Jika dikaitkan dengan Pasal 27 ayat (1) UU ITE, aturan ini bisa diterapkan ketika deepfake diproduksi dan disebarkan dalam bentuk yang tidak sopan atau melanggar kesusilaan. Pasal 27 A UU ITE bisa digunakan sebagai dasar hukum yang tepat ketika deepfake digunakan untuk menyerang kehormatan nama baik seseorang. Secara normatif pasal ini mengatur perbuatan menyerang kehormatan dengan cara mengatakan sesuatu yang salah agar banyak orang tahu melalui televisi atau internet.[5] Dalam praktiknya ketentuan ini memang terlihat cocok digunakan untuk kasus deepfake yang menampilkan korban seolah-olah melakukan tindakan tercela.

Pasal 28 ayat (1) UU ITE yang mengatur perbuatan menyebarkan berita palsu dan menyesatkan yang menyebabkan kerugian bagi konsumen dalam transaksi elektronik. Pasal imi memuat unsur "setiap orang" dengan sengaja dan tanpa hak "menyebarkan berita bohong" dan menyesatkan serta mengakibatkan kerugian konsumen dalam transaksi elektronik (UU) ITE pasal 28 ayat (1) unsur "setiap orang" mencakup individu maupun badan hukum sebagai subjek hukum yang dapat dipertanggng jawabkan secara pidana, sedangkan unsur "dengan sengaja" menunjukan bahwa pelaku memiliki keinginan dan kesadaran terhadap akibat dari perbuatannya bukan sekedar kelalaian.[6]

Dalam kasus polda jatim, para tersangka dihadapkan pada dua pasal alternatif UU ITE. Pertama, Pasal 51 ayat (1) bersamaan dengna Pasal 35 UU ITE mengatur pemalsuan

[3] Abdurrauf Law, "1 1* 1" 1, no. 2 (2024): 22–38.
[4] Ika F. Muhamad A., M. Rizan, "Journal of S Ocial and Economics Research," *Jurnal Sosial Dan Ekonomi* 3(2), no. 1 (2025): 123–38.
[5] I Putu Gede Aryawan, "Kekosongan Norma Hukum Dalam Penanganan Deepfake Sebagai Alat Kejahatan Siber : Studi Yuridis Di Wilayah Polri Klungkung" 2, no. April (2026): 295–307.
[6] Jurnal Riset and Multidisiplin Edukasi, "ANALISIS PENGATURAN HUKUM TINDAK PIDANA CYBER CRIME PHISING" 3 (2026): 1216–30.

dokumen atau informasi elektronik. Pasal 35 menyatakan bahwa "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubah, penghilangan, pengrusakan informasi Elektronik dan atau dokumen elektronik dengan tujuan agar informasi elektronik atau dokumen elektronik terbukti palsu atau secara langsung berkaitan dengan praktik pembuatan video deepfake.

Ada jenis malware lain yang menggunakan algoritma deepfake, seperti pencurian identitas, Dimana seseorang menggunakan video dan suara palsu untuk mencemarkan nama baik dan menipu orang lain.[7] Teknologi modifikasi suara/audio Adalah bagian dari AI yang memiliki kemampuan untuk mengubah suara dengan menggunakan algoritma yang bertujuan untuk mengubah suara sesuai keinginan. Teknologi deepfake mengancam privasi. Deepfake dapat digunakan untuk melakukan pemerasan atau mencemarkan nama baik seseorang karena kemampuan mereka untuk membuat konten visual dan audio yang sangat realistis sebagai contoh, seseorang dapat membuat video deepfake yang menampilkan orang dalam situasi kompromi dan mengancam untuk menyebarkannya kecuali syarat tertentu dipenuhi.

Teknologi deepfake semakin mudah digunakan oleh siapa saja dan Dimana saja dengan jenis apa saja, terasul mereka yang tidak memiliki teknis yang kuat yang memperparah masalah privasi ini. Sebaliknya, ada kekurangan perlindungan hukum substantif dan prosedural untuk korban kejahatan deepfake.

Karena aparat hukum tidak memahami modus deepfake, korban sering mengalami trauma psikologis, kerugian social, dan kesulitan untuk mendapatkan keadlian. Dalam hal keadilan dan hak asasi manusia negara seharusnya memberikan perlindungan hukum yang efektif terhadap korban, baik preventif maupun represif, melalui mekanisme hukum yang berperspektif pada korban.[8] Korban kejahatan deepfake sering kali menghadapi kesulitan dalam memperoleh keadilan dan pemulihan hak psikologis dan hukum. Dalam

[7] Silvia Maharani Iskandar Putri, Nashwa Salsabila, and Asmak Ul Hosnah, "Jurnal Hukum Legalita Kriminalisasi Penggunaan Deepfake Dalam Tindak Pidana Penipuan," *Jurnal Hukum Legalita* 6, no. 2 (2023): 83–90.

[8] Puspitasari Gustami and Devi Siti Hamzah Marpaung, "Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.1. No.4 (Juli 2020) Tema/Edisi : Hukum Pidana (Bulan Ketujuh) Https://Jhlg.Rewangrencang.Com/," *Rewang Rencang : Jurnal Hukum Lex Generalis* 1, no. 4 (2020): 1–12.

banyak kasus, korban menghadapi hambatan structural dan social. Seperti kurangnya pemahaman aparat hukum tentang teknologi ini dan stigma yang melekat karena konten palsu yang tersebar luas.

Deepfake menggunakan algoritma deep learning, salah satu model machine learning yang paling populer adalah Generaitve Adversarial Networks (GANs), untuk merekayasa konten dalam bentuk gambar maupun video. GAN terdiri dari dua bagian utama yaitu generator dan discriminator.[9] Kedua komponen ini berkerja secara bersaing dalam proses pembelajaran dimana generator terus belajar untuk menghasilkan data yang semakin mirip dengan data asli sementara discriminator bertanggung jawab untuk membedakan antara data asli dan data yang dibuat oleh generator

Dampak dari penipuan ini cukup signifikan, baik dari segi finansial maupun sosial. Banyak korban yang tertipu dan mentransfer sejumlah uang dengan harapan mendapatkan bantuan yang dijanjikan. Menurut laporan pelaku berhasil mengumpulkan puluhan juta rupiah dari korban korbanya dalam kurun waktu beberapa bulan. Kerugian finansial ini menunjukan bagaimana teknologi deepfake dapat dimanfaatkan untuk mengeksploitasi kepercayaan masyarakat, terutama dalam situasi yang melibatkan tokoh publik dan janji bantuan keuangan.

Penipuan semacam ini memiliki konsekuensi psikologis dan sosial yang signifikan selain kerugian materi. Kepercayaan masyarakat terhadap informasi resmi terguncang, dan banyak korban mengalami tekanan emosional karena merasa tertipu. Pada akhirnya komunikasi pemerintah atau lembaga resmi dapat terhambat karena masyarakat menjadi lebih skeptis. Akibatnya tindakan pencegahan yang lebih ketat diperlukan, seperti meningkatkan kesadaran publik tentang deepfake dan memperkuat undang-undang untuk mencegah penyalahgunaan teknologi ini.

Peran Edukasi Masyarakat dalam pencegahan penipuan Deepfake meningkatkan kesadaran publik dan edukasi adalah langkah pertama dan terpenting dalam pencegahan deepfake. Masyarakat harus memahami apa itu deepfake, bagaimana itu bekerja dan

[9] Yoan Shevila Kristiyenda, Jasmine Faradila, and Christina Basanova, "Pencegahan Kejahatan Deepfake: Studi Kasus Terhadap Modus Penipuan Deepfake Prabowo Subianto Dalam Tawaran Bantuan Uang," *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (2025): 149–64, https://doi.org/10.59246/aladalah.v3i2.1263.

bahayanya. Kampanye literasi digital dapat membantu orang menjadi lebih kritis terhadap apa yang mereka lihat dan bagikan di media sosial. Selain itu, penting bagi jurnalis, penegak hukum dan profesional terkait lainya untuk menerima pelatihan khusus untuk mengidentifikasi dan menanggapi deepfake dengan tepat.[10]

Pengembangan teknologi untuk mendeteksi deepfake adalah bagian penting dari pencegahan. Para peneliti dan perushaan teknologi harus mengembangkan alat dan algoritma yang dapat mendeteksi deepfake dengan tingkat akurasi yang tinggi. misalnya, analisis forensik digital, pembelajaran mesin, dan kecerdasan buatan digunakan untuk mengidentifikasi anomali yang tidak biasa dalam rekaman audio dan video. Deteksi otomatis ini dapat dimasukkan ke dalam penuyedia layanan internet dan platform media sosial untuk memantau dan menghapus konten deepfake sebelum menyebar luas.

Penggunaan AI harus melindungi data pribadi dari ancaman seperti video deepfake. Data pribadi termasuk foto diri harus dilindungi sesuai dengan undang-undang. Privasi fisik, informasi dan organisasi mencakup perlindungan terhadap komunikasi, tindakan, dan identitas individu. Orang-orang di eropa memiliki kemampuan untuk menggunakan hak "right to be forgotten" (RTBF) untuk menghapus informasi pribadi dari internet.

2. Hambatan yuridis dan non yuridis yang dihadapi dalam penegakan hukum terhadap pelaku penipuan deepfake berdasrakan Pelajaran dari kasus Polda Jatim

Dalam kasus penipuan deepfake AI dari kasus polda jaya kasus ini dimulai dengan laporan yang dibuat oleh staf dinas kominfo Jawa Timur pada tanggal 14 dan 15 April 2025 tentang akun tiktok yang mencurigakan yang menyebarkan video manipulative yang mencatut nama gubernur Jawa Timur, dengan nama akun: @khofiggh75g, @khofiljatim, @khofifahnew, dan @khofiaindah di antaranya. Segera setelah itu direktorat reserse siber Polda Jatim melakukan patrol siber dan menemukan tiga tersangka, yang masing-masing memiliki peran sebagai berikut:

Tersangka	Usia	Peran	Keterangan

[10] Adnasohn Aqilla Respati et al., "Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban," *Media Hukum Indonesia* 2, no. 2 (2024): 586–92, https://doi.org/10.5281/zenodo.12508126.

HMP	32 TH	Pembuatan akun TikTok dan editor video deepfake menggunakan AI	Pembuat konten utama menyerahkan video kepada UP
UP	24 TH	Penyedia rekening bank untuk menampung dana hasil penipuan	Rekening atas nama Maharani
AH	34 TH	Admin Whatsapp mengelabui korban agar melakukan transfer	Operator Komunikasi dengan korban

Tabel 1. Identitas dan peran Tersangka Kasus Deepfake Polda Jatim (April 2025)

a) Hambatan Yuridis

Hambatan atau kendala utama dalam penegakan hukum terhadap penipuan deepfake adalah:

- Dalam teori kepastian hukum, Gustav Radbruch menyebutkan empat hal yang berkaitan dengan nilai kepastian hukum. Pertama, hukum haruslah positif, artinya hukum itu sendiri merupakan peraturan perundang-undangan. Kedua hukum harus didasarkan pada fakta yang nyata. ketiga, hulkum tidak hanya harus mudah dilaksanakan, tetapi juga harus dirumuskan dengan jelas agar tidak menimbulkan perbedaan penafsiran. Keempat, hukum tidak boleh diubah dengan mudah atau sering. Menurut Gustav Raddbruch, kepastian hukum adalah kepastian tentang hukum itu sendiri, yang mencakup permasalahan atau perkara hukum dalam masyarakat. Oleh karena itu, kepastian hukum harus selalu ditaati, meskipun hukum positif atau perundang-undangan dianggap kurang adil.

Kekosongan regulasi khusus atau legal vacuum: undang-undang di indonesia belum mengatur deepfake sebagai tindak pidana tersendiri. Pasal-pasal UU ITE saat ini umum dan tidak dapat menangani kekompleksan fitur deepfake, terutama dalam hal pembuktian teknis. Karena UU ITE secara fundamental mengatur masalah digital secara keseluruhan, penggunaan AI dapat dikategorikan sebagai agen elektronik dalam UU ITE. Namun, UU

ITE belum cukup untuk menangani masalah yang ditimbulkan oleh perkembangan AI yang cepat.[11]

Saat ini, Indonesia sedang berusaha untuk membuat aturan yang lebih spesifik tentang kecerdasan artifisial, yaitu Strategi Nasional Kecerdasan Artifisial Indonesia atau Stranas KA.[12] Akibat dari tidak adanya undang-undang yang mengatur secara spesifik mengenai kejahatan deepfake yaitu muncul tantangan dalam menentukan konstruksi hukum yang paling tepat karena deepfake merupakan bentuk kejahatan baru yang memadukan manipulasi identitas, teknologi AI, dan penipuan digital.

- Problematika Pembuktian Digital: Hukum acara pidana di Indonesia masih belum bisa sepenuhnya menerima bukti digital yang menggunakan teknologi kecerdasan buatan. Apakah bukti elektronik bisa diterima atau tidak, masih tergantung pada pendapat hakim yang berbeda-beda. Teknologi deepfake membuat kita bisa memanipulasi gambar dan video kita jadi sulit membedakan mana yang asli dan mana yang palsu. Hal ini merusak nilai orsisinalitas karya asli. Pasalnya, hasil deepfake bisa terlihat sangat meyakinkan, kondisi ini makin parah dengan maraknya informasi palsu atau hoax. Masyarakat kini sulit membedakan antara fakta dan fiksi. Akibatnya, keprcayaan masyarakat pada informasi menurun bahkan, ketidak pastian informasi yang beredar di media meningkat.[13] Penerapan AI ternyata menimbulkan maslah baru dalam digital forensics. misalnya , dokumen yang dihasilkan oleh chatGPT sering kali tidak memiliki metadata asli. Hal ini karena AI generatif dapat membuat data dari awal, bukan dengan mengedit file yang sudah ada, kini dokumen palsu dapat terlihat sangat mirip dengan dokumen asli. Ini menjadi tantangan besar

[11] Ezra Pranata Tarigan and I Nyoman Prabu Buana Rumiartha, "Kekosongan Hukum AI Di Indonesia: Kasus Deepfake Terhadap Sri Mulyani Dan Perbandingan EU AI Act," *Jurnal Media Akademik (JMA)* 3, no. 11 (2025): 1–19.

[12] Adnasohn Aqilla Respati, "Reformulasi Undang-Undang ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation Reformulation of the ITE Law on Artificial Intelligence Compared to the European Union and China AI Act Regulation," *Jurnal USM Law Review* 7, no. 3 (2024): 4–12.

[13] Ira Febriana and Shifa Intan Rahma, "Analisis Kebijakan UU Nomor 1 Tahun 2024 (Untuk Penanganan Cyber Bullying) Dengan Perspektif Problem Tree Analysis," *Journal of Research and Development on Public Policy* 3, no. 2 (2024): 113–23, https://doi.org/10.58684/jarvic.v3i2.144.

bagi penyedik untuk membuktikan bahwa dokumen tersebut palsu di pengadilan. Penyidik tidak bisa hanya mengandalkan alat deteksi manipulasi gambar standar.[14]

- Kelemahan definisi yuridis adalah bahwa belum ada definisi hukum yang lengkap tentang deepfake dalam peraturan perundang-undangan di Indonesia. Hal ini menyebabkan ketidakjelasan dalam menerapkan unsur-unsur tindak pidana yang terkait dengan deepfake. Dengan tidak adanya definis yang jelas, sulit untuk menentukan apa yang termasuk dalam kategori deepfake dan bagaimana cara menanganinya secara hukum ini membuat penerapan hukum menjadi tidak konsisten dan dapat menimbulkan masalah dalam penegakan hukum.

Oleh karena itu, perlu ada upaya untuk membuat definisi hukum yang komprehensif tentang deepfake dalam peraturan perundang-undangan Indonesia, sehingga dapat membantu menjelaskan dan menyelesaikan masalah yang terkait dengan deepfake.

b) Hambatan Non Yuridis

Diluar aspek regulasi, terdapat sejumlah hambatan non yuridis yang tidak kalah krusial:

- Keterbatasna kapasitas teknis penyidik: investigasi kasus deepfake memerlukan keahlian khusus dalam bidang forensik digital, machine learning, dan analisis mendata yang belum merata diseluruh satuan siber polri
- Kecepatan perkembangan teknologi: Algoritma deepfake terus berkembang dengan pesat sehingga metode deteksi yang ada hari ini dapat menjadi usang dalam hitungan bulan. Kecerdasan alami akan cepat mengalami perubahan. Hal ini dimungkinkan karena kemampuan manusia unutk mengingat sesuatu cukup terbatas. Kecerdasan buatan tidak akan berubah selama sistem komputer dan program tidak diubah.[15]
- Rendahnya literasi digital masyarakat: rendahnya kemampan masyarakat dalam memahami dan mengunakan media sosial menjadi salah satu pemyebab utama yang membuat masyarakat rentan terhadap konten palsu. Literasi media sosial kemampuan seseorang untuk memahami, menganalisis, dan menilai pesan digital secara alami.

[14] Abid Juandana and Lolita Fitriyana, "Analisis Yuridis Pertanggungjawaban Tindak Pidana Penipuan Dengan Modus Pemalsuan Dokumen Digital Menggunakan ChatGPT" 10, no. 1 (2026): 112–23.
[15] Persetujuan Disertasi, *MENGGUNAKAN ARTIFICIAL INTELLIGENCE*, 2025.

Masyarakat yang memiliki literasi rendah cenderung mempunyaiinformasi tanpa memeriksa kebenaranya dan mudah tergoda oleh konten yang dikembangkan untuk mempengaruhi pikiran seperti deepfake atau voice cloning. Tingkat kemampuan mengidentifikasi konten deepfake masih sangat rendah, sehingga korban mudah tertipu oleh konten manipulatif yang tampak meyakinkan.

- Minimnya kerjasama platform digital: platform media sosial seperti Tiktok, Whatsapp belum memiliki mekanisme yang cepat dan efektif untuk mendeteksi serta menghapus konten deepfake berbahaya.
- Kurangnya kordinasi Antar lembaga: dari segi kelembagaan dan sumber daya manusia, penenlitian oleh Atho'hillah (2025) menunjukan bahwa kemampuan para petugas hukum seperti penyidik, jaksa, dan hakim dalam memahami struktur AI, pola serangan yang sangat cerdas, serta teknik pembukitan forensik berdasarkan algoritma masih kurang memadai dan tergolong tertinggal dibandingkan perkembangan inovasi yang dilakukan pelaku.[16] Penanganan kejahatan deepfake memerlukan kordinasi antara polri, kominfo (kini komdig), OJK, dan lembaga terkait lainnya, namun protokol koordinasi lintas lembaga masih belum optimal.

3. Rekomendasi optimalisasi penegakan hukum terhadap penipiuan deepfake AI di Indonesia

a) Reformulasi Regulasi

Deepfake yang berupa penipuan identitas digital bisa terlihat seperti salah satu tindak kriminal, dan hal ini merupakan tindakan pidana yang dapat menyebabkan trauma psikologis yang sangat dalam pada korban.[17] Rekomendasi jangka pendek yang bisa dilakukan segera adalah dengan menerbitkan peraturan pemerintah atau peraturan menteri yang lebih spesifik mengenai deepfake, sebagai bagian dari penerapan Undang-

[16] M. Effendy, " Tantangan Penegakan Hukum Terhadap Kejahatan Siber.," *Jurnal Hukum & Teknologi,* 7, no. 1 (2022): 45–60.

[17] Hazmin Sulton Firdaus and Lona Puspita, "Peran Hukum Dalam Mengatasi Penyebaran Konten Deepfake Untuk Penipuan Identitas Digital," *UIR Law Review* 9, no. 1 (2025): 1–14, https://journal.uir.ac.id/index.php/uirlawreview/article/view/22095.

undang ITE. pada jangka menengah diperlukan perubahan dalam Undang-undang ITE agar mendefinisikan dan menentukan syarat hukum terkait deepfake secara jelas.

Jangka panjangnya, Indonesia perlu mengenang pembuatan Undang-undang tentang kecerdasan buatan (AI Act Indonesia) yang lengkap, yang mencakup empat hal utama: Pertama, menentukan arti dan jenis sistem AI berdasarkan tingkat bahayanya. Kedua, memastikan transparansi dan penandatanganan konten AI. Ketiga, menetapkan standar bukti digital untuk konten yang menggunakan Ai. Serta Keempat memberikan hukuman yang sesuai jika teknologi AI digunakan dengan cara yang tidak benar.

b) Peningkatan Kapasitas Penegak Hukum

Banyak organisasi internasional dan kelompok ahli telah membuat pedoman tentang cara menangani bukti digital, yang fokus pada prinsip ketpatan, kepercayaan, dan tanggung jawab dalam setiap tahap proses penyelidikan forensik.[18] Polri, khususnyaa Direktorat Siber harus meningkatkan kemampuan dalam penyelidikan digital dengan cara memberikan pleatihan terus menerus kepada petugas siber tentang teknologi mendeteksi deepfake.

Membangun laboratorium forensik digital yang dilengkapi dengan perangkat lunak terbaru untuk mendeteksi deepfake lalu berkerja sama dengan perguruan tinggi dan lembaga penelitian untuk mengembangkan metode penyelidikan deepfake yang bisa beradaptasi dengan perkembangan teknologi.

c) Kolaborasi Multipihak

Penegakan hukum terhadap deepfake tidak bisa hana dilakukan sendirain oleh pihak berwajib saja. Diperlukan kolaborasi yang melibatkan:

- Pemerintah akan memperkuat aturan kerja antar kementerian atau lembaga, serta memberikan dana yang cukup untuk meningkatkan kemampuan siber.

[18] Mozaik Desa, Pematang Serai, and Langkat Perspektif, "NUSANTARA : Jurnal Ilmu Pengetahuan Sosial ى ل ةتلا و ع ل ا و اون وا ب ل ات و ى و ق ر ع الل اون وا ث ل ا ى ل ع ن ت د ع لا و م ع دي د ش ب ا ق ع," *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 9, no. 4 (2022): 1483–90.

- Platform Digital wajib melakukan pemantauan dan penghapusan konten deepfake yang berbahaya, menyediakan sistem pelaporan yang mudah digunakan oleh pengguna, serta berkerja sama aktif dengan pihak berwajib dalam menegakan hukum
- Masyarakat sipil akademis dengan program literasi digital nasional, penelitian terus menerus mengenai dampak dan cara mengatasi deepfake, serta advokasi kebijakan yang didasarkan pada bukti.
- Komunitas Internasional memperkuat kerjasama antar negara dalam mengatasi kejahata siber yang terjadi lintas batas, seperti kesepakatan ekstradisi dan bantuan hukum bersama.

d) Peningkatan Literasi Digital Masyarakat

Karena masyarakat masih kurang mampu mengenali konten deepfake, maka penting bagi pemerintah untuk membuat program pengajaran ke publik yang besar dan teratur sebagai prioritas utama. Program ini bisa diintegrasikan ke dalam kurikulum pendidikan resmi, kampanye media sosial yang dijalankan pemerintah, serta kegiatan penyuluhan hukum dikalangan komunitas yang rentan. Masyarakat harus diajarkan untuk selalu memeriksa informasi dari sumber yang sah sebelum menerima konten yang melibatkan tokoh publik, terutama yang menyertakan penawaran keuangan. Dengan cara ini, program pelatihan ini dapat digunakan sebagai contoh untuk memberdayakan masyarakat melalui literasi digital yang dapat diterapkan di desa-desa.[19]

4. KESIMPULAN DAN SARAN

Berdasarkan pembahasan diatas, tiga kesimpulan utama dapat diambil. Pertama, hukum positif di Indonesia, Khususnya UU No. 1 Tahun 20024 tentang ITE dan KUHP, pada dasarnya mampu menjangkau pelaku penipuan deepfake melalui pasal-pasal umum mengenai manipulasi data elektronik, penyebaran informasi tidak benar, dan penipuan. Hal ini terbkti dari keberhasilan Polda Jatim dalam menerapkan Pasal 51 ayat (1) dan Pasal 45A ayat (1) UU ITE pada kasus deepfake yang melibatkan Gubernur Jatim.

[19] Cindy Atika Rizki et al., "Peningkatan Literasi Digital Masyarakat Melalui Pelatihan Pemanfaatan Google Workspace," *Jurnal Pengabdian Masyarakat Berdampak* 1, no. 1 (2025): 29–36, https://doi.org/10.64803/jupemba.v1i1.35.

Namun, ketiadaan peraturan yang secara langsung mengatur tentang deepfake menciptakan celah hukum yang bisa menghambat penanganan kasus yang lebih rumit.

Kedua, penerapan hukum terhadap penipuan deepfake menghadapi berbagai tantangan dari segi yuridis terdapat masalah karena tidak adanya hukum yang jelas, kesulitan dalam pemuktian digital, dan kemungkinan masalah yuridiksi, sedangkan dari segi non yuridis meliputi keterbatasan kemampuan teknis penyidik, rendahnya pemahaman digital dalam masyarakat, dan kurangnya kerjasama dengan platform digital.

Ketiga, untuk mengoptimalkan penerapan hukum diperlukan pendekatan yang menyeluruh, yang meliputi reformulasi regulasi, peningkatan kapasitas aparat penegak hukum, kolaborasi antar pihak yang sejalan, serta penguatan literasi digital di masyarakat secara berkesinambungan.

DAFTAR REFERENSI

Aryawan, I Putu Gede. "Kekosongan Norma Hukum Dalam Penanganan Deepfake Sebagai Alat Kejahatan Siber : Studi Yuridis Di Wilayah Polri Klungkung" 2, no. April (2026): 295–307.

Desa, Mozaik, Pematang Serai, and Langkat Perspektif. "NUSANTARA : Jurnal Ilmu Pengetahuan Sosial ىلٗ تلاوَعَلاوَاوُنواِبِلاَتوَىوَقَرَعاللٗاوُنواِثلااىَلْ ىلٗ تلاوَعَلاوُنواِبِلاَتوَىوَقَرَعاللٗاوُنواِثلااىَلْ عٗنَتَدُعلاوَمَعٗديِدشبِاَقع." *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 9, no. 4 (2022): 1483–90.

Disertasi, Persetujuan. *MENGGUNAKAN ARTIFICIAL INTELLIGENCE*, 2025.

Effendy, M. " Tantangan Penegakan Hukum Terhadap Kejahatan Siber." *Jurnal Hukum & Teknologi,* 7, no. 1 (2022): 45–60.

Firdaus, Hazmin Sulton, and Lona Puspita. "Peran Hukum Dalam Mengatasi Penyebaran Konten Deepfake Untuk Penipuan Identitas Digital." *UIR Law Review* 9, no. 1 (2025): 1–14. https://journal.uir.ac.id/index.php/uirlawreview/article/view/22095.

Gustami, Puspitasari, and Devi Siti Hamzah Marpaung. "Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.1. No.4 (Juli 2020) Tema/Edisi : Hukum Pidana (Bulan Ketujuh) Https://Jhlg.Rewangrencang.Com/." *Rewang Rencang : Jurnal Hukum Lex Generalis* 1, no. 4 (2020): 1–12.

Ira Febriana, and Shifa Intan Rahma. "Analisis Kebijakan UU Nomor 1 Tahun 2024 (Untuk Penanganan Cyber Bullying) Dengan Perspektif Problem Tree Analysis." *Journal of Research and Development on Public Policy* 3, no. 2 (2024): 113–23. https://doi.org/10.58684/jarvic.v3i2.144.

Juandana, Abid, and Lolita Fitriyana. "Analisis Yuridis Pertanggungjawaban Tindak Pidana Penipuan Dengan Modus Pemalsuan Dokumen Digital Menggunakan ChatGPT" 10, no. 1 (2026): 112–23.

Kristiyenda, Yoan Shevila, Jasmine Faradila, and Christina Basanova. "Pencegahan Kejahatan Deepfake: Studi Kasus Terhadap Modus Penipuan Deepfake Prabowo Subianto Dalam Tawaran Bantuan Uang." *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (2025): 149–64. https://doi.org/10.59246/aladalah.v3i2.1263.

Law, Abdurrauf. "1 1* 1" 1, no. 2 (2024): 22–38.

Muhamad A., M. Rizan, Ika F. "Journal of S Ocial and Economics Research." *Jurnal Sosial Dan Ekonomi* 3(2), no. 1 (2025): 123–38.

Putri, Silvia Maharani Iskandar, Nashwa Salsabila, and Asmak UI Hosnah. "Jurnal Hukum Legalita Kriminalisasi Penggunaan Deepfake Dalam Tindak Pidana Penipuan." *Jurnal Hukum Legalita* 6, no. 2 (2023): 83–90.

Respati, Adnasohn Aqilla. "Reformulasi Undang-Undang ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation Reformulation of the ITE Law on Artificial Intelligence Compared to the European Union and China AI Act Regulation." *Jurnal USM Law Review* 7, no. 3 (2024): 4–12.

Respati, Adnasohn Aqilla, Astri Dewi Setyarini, Dodi Parlagutan, Muhammad Rafli, Rayhan Syahbana Mahendra, and Andriyanto Adhi Nugroho. "Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban." *Media Hukum Indonesia* 2, no. 2 (2024): 586–92. https://doi.org/10.5281/zenodo.12508126.

Riset, Jurnal, and Multidisiplin Edukasi. "ANALISIS PENGATURAN HUKUM TINDAK PIDANA CYBER CRIME PHISING" 3 (2026): 1216–30.

Rizki, Cindy Atika, Mardiah, Eka Pandu Cynthia, Alabbas Hussein Saeed, and Nabila Khairuniza. "Peningkatan Literasi Digital Masyarakat Melalui Pelatihan Pemanfaatan Google Workspace." *Jurnal Pengabdian Masyarakat Berdampak* 1, no. 1 (2025): 29–36. https://doi.org/10.64803/jupemba.v1i1.35.

Tarigan, Ezra Pranata, and I Nyoman Prabu Buana Rumiartha. "Kekosongan Hukum AI Di Indonesia: Kasus Deepfake Terhadap Sri Mulyani Dan Perbandingan EU AI Act." *Jurnal Media Akademik (JMA)* 3, no. 11 (2025): 1–19.

Sumber Berita dan Laman Resmi

Dinas Komunikasi dan Informatika Provinsi Jawa Timur. "Polda Jatim Ungkap Kasus Penipuan Deepfake AI Kepala Daerah, Pelaku Kantongi Keuntungan Hingga Rp87 Juta." 28 April 2025. https://kominfo.jatimprov.go.id

DetikJatim. "Pelaku Penipuan Deepfake Khofifah Raup Untung Rp 87 Juta Selama 3 Bulan." 29 April 2025. https://news.detik.com

SIP Law Firm. "Pidana atas Konten Deepfake, Tantangan Baru Penegakan Hukum di Era AI." 11 Agustus 2025. https://siplawfirm.id

Liputan6. "Modus Penipuan Deepfake Naik 1.550 Persen di Indonesia." 2 November 2024. https://liputan6.com