PERSPEKTIF HUKUM

Volume 26 Issue 1 Mei 2026

TANGGUNG JAWAB HUKUM ATAS PENYALAHGUNAAN TEKNOLOGI *AI*: STUDI KASUS *DEEPFAKE* PRABOWO SUBIANTO DALAM MODUS BANTUAN UANG

Sofia [1], Rina Shahriyani Shahrullah [2], Ampuan Situmeang [3]

[1] Universitas Internasional Batam, Indonesia, Email: 24.sofia@uib.edu
[2] Universitas Internasional Batam, Indonesia, Email: rina@uib.ac.id
[3] Universitas Internasional Batam, Indonesia, Email: ampuan.situmeang@uib.ac.id

✉ corresponding email: 24.sofia@uib.edu

Article

Keywords:
Deepfake Artificial Intelligence, Digital Fraud, Criminal Liability

Article History
Received: Jan 23, 2026;
Reviewed: May 26, 2026;
Accepted: May 28, 2026;
Published: Jun 04, 2026;

Abstract

The development of deepfake artificial intelligence technology poses new challenges for Indonesian criminal law because it can be used to digitally manipulate a person's face, voice, and identity. This study aims to analyze the modus operandi of deepfake AI technology abuse as well as the legal liability of perpetrators in digital fraud crimes. This study employs a normative legal research method using a statutory approach, a case-based approach, and a conceptual approach. The results indicate that the modus operandi of deepfake misuse involves the dissemination of AI-generated manipulative videos featuring President Prabowo Subianto, purporting to offer financial assistance to the public, accompanied by a WhatsApp number to direct victims to communicate with the perpetrator and transfer funds. Legal liability in this case arises because the perpetrator's actions satisfy the elements of a criminal offense: there is intent, the perpetrator possesses the capacity to be held accountable, and no justifying or exculpatory grounds are found. This criminal liability is based on Article 51(1) in

conjunction with Article 35 of the ITE Law and Article 378 of the Criminal Code, while the PDP Law is used as a supporting normative instrument in addressing the misuse of digital identities in the form of faces and voices. This study underscores the importance of strengthening regulations, digital evidence, and harmonizing legal frameworks regarding the misuse of deepfake technology.

https://doi.org/10.30649/ph.v26i1.550

Pendahuluan

Teknologi *deepfake* telah menjadi salah satu inovasi paling mencolok dalam perkembangan *Artificial Intelligence* (*AI*), memanfaatkan algoritma *Generative Adversarial Networks* (GAN) untuk menciptakan konten visual dan audio yang sulit dibedakan dari kenyataan.[1] Pertumbuhan pengguna *AI* pada tahun 2024, jumlah pengguna *AI* di Indonesia diperkirakan mencapai 1,3 juta pengguna, dengan proyeksi peningkatan hingga 3,33 juta pada tahun 2030.[2] *AI* menjadi kian populer, Indonesia masuk daftar 10 peringkat teratas sebagai pengguna *AI* terbanyak sepanjang periode bulan September 2022 hingga Agustus 2023.[3] Peningkatan penggunaan AI tersebut tidak hanya menunjukkan kemajuan teknologi, tetapi juga menimbulkan konsekuensi hukum apabila teknologi tersebut disalahgunakan untuk merugikan orang lain. Dalam konteks hukum pidana, kemudahan akses terhadap AI dapat membuka peluang

[1] Rendi Syaputra, "Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artificial Inteligence (AI) Dari Perspektif Hukum Pidana Indonesia," *Jurnal Hukum Respublica*, 2024, 1–13, https://doi.org/https://doi.org/10.31849/respublica.v24i01.23327.

[2] Garuda, "Data Pengguna AI Di Indonesia Update Terbaru," 2025, https://www.garuda.website/blog/data-pengguna-ai-indonesia/.

[3] GoodStats, "10 Negara Pengguna AI Terbanyak, Indonesia Salah Satunya," GoodStats, 2024, https://data.goodstats.id/statistic/10-negara-pengguna-ai-terbanyak-indonesia-salah-satunya-RLlmC.

terjadinya tindak pidana digital dengan modus yang semakin sulit dideteksi, salah satunya melalui penyalahgunaan teknologi *deepfake*.

Perkembangan teknologi AI, khususnya deepfake, menimbulkan persoalan hukum baru dalam hukum pidana Indonesia karena dapat digunakan untuk memanipulasi wajah, suara, dan identitas seseorang secara digital.[4] Persoalan hukum yang muncul tidak hanya berkaitan dengan penyebaran konten palsu, tetapi juga menyangkut pemenuhan unsur tindak pidana, pembuktian atas keaslian informasi elektronik, penyalahgunaan identitas digital, serta pertanggungjawaban pidana pelaku. Polri bahkan memprediksi bahwa *deepfake* akan menjadi salah satu tren serangan di dunia siber pada 2025.[5] Kementerian Komunikasi dan Digital (Komdigi) juga mengeluarkan imbauan agar masyarakat waspada terhadap aksi kriminalitas dan penipuan berbasis *AI*.[6] Data industri menegaskan urgensi tersebut PT VIDA (*Digital Identity Indonesia*) mencatat lonjakan kasus penipuan *deepfake* sebesar 1.550% pada 2022–2023. [7] Kondisi ini menunjukkan bahwa tindak pidana digital semakin kompleks, terutama ketika teknologi *deepfake*

[4] Cleophila Nathania Putri Hernawan, Debby Telly Antow, and Arie Sendow, "Tinjauan Hukum Mengenai Penyalahgunaan Artificial Intellingence Dalam Tindak Pidana Kekerasan Seksual," *Lex Privatum Jurnal Fakultas Hukum Unsrat* 15, no. 4 (2025): 12, https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/61860.

[5] Pusiknas Bareskrim Polri, "Tim Siber Ungkap Teknologi Deepfake Catut Nama Pejabat Negara," *Pusiknas Bareskrim Polri*, January 31, 2025, https://pusiknas.polri.go.id/detail_artikel/tim_siber_ungkap_teknologi_deepfake_catut_nama_pejabat_negara.

[6] Biro Humas Kementerian Komdigi, "Marak Penipuan Dengan AI, Wamenkomdigi Nezar Patria Minta Masyarakat Waspada," *Komdigi*, April 13, 2025, http://komdigi.go.id/berita/siaran-pers/detail/marak-penipuan-dengan-ai-wamenkomdigi-nezar-patria-minta-masyarakat-waspada.

[7] VIDA Digital Identity, "Penipuan Deepfake Indonesia Melonjak 1550%: Begini Cara VIDA Memeranginya," *VIDA Digital Identity*, October 2024, https://vida.id/id/pressrelease/penipuan-deepfake-indonesia-melonjak-1550-begini-cara-vida-memeranginya.

digunakan dalam modus penipuan, penyebaran hoaks, maupun pencemaran nama baik. [8]

Kondisi tersebut menunjukkan bahwa penyalahgunaan *deepfake* tidak cukup dipahami sebagai persoalan teknologi semata, tetapi perlu ditempatkan sebagai isu hukum pidana. Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) memberikan dasar hukum yang lebih kuat dalam menangani masalah tindak pidana digital, termasuk penyalahgunaan teknologi *deepfake*. UU ITE menjadi dasar untuk menilai perbuatan manipulasi Informasi Elektronik dan/atau Dokumen Elektronik, sedangkan UU PDP relevan dalam melihat penyalahgunaan identitas digital berupa wajah dan suara. Penyalahgunaan teknologi *deepfake* di Indonesia telah menunjukkan dampak yang sangat nyata dan semakin meningkat. Laporan penegak hukum menunjukkan peningkatan tajam tindak pidana digital dalam beberapa tahun terakhir.

Tabel 1. Data Jumlah Laporan Tindak Pidana Digital Mengalami Kenaikan dalam 3 Tahun Terakhir

2022	2023	2024	2025 (s.d. 23 Jan)
Jumlah Laporan	Jumlah Laporan	Jumlah Laporan	Jumlah Laporan

[8] Agus Wibowo and Sri Yulianingsih, *Hukum Teknologi Informasi*, *Yayasan Prima Agus Teknik Bekerja Sama Dengan Universitas Sains & Teknologi Komputer (Universitas STEKOM)* (Semarang: Yayasan Prima Agus Teknik Bekerja sama dengan Universitas Sains & Teknologi Komputer (Universitas STEKOM), 2025), https://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/578.

8.636 Perkara	11.297 Perkara	13.913 Perkara	1.062 Perkara

Sumber: Pusiknas Bareskrim Polri[9]

Berdasarkan data di atas, terlihat adanya peningkatan yang signifikan dalam jumlah laporan tindak pidana digital di Indonesia dalam tiga tahun terakhir. Peningkatan tajam ini menunjukkan bahwa tindak pidana digital, yang kini banyak melibatkan teknologi canggih seperti *deepfake*, semakin menjadi masalah serius. Di Indonesia, penyalahgunaan teknologi *deepfake* telah muncul dalam bentuk penipuan digital yang mencatut tokoh publik. Salah satu perkara yang dikaji adalah Putusan Pengadilan Negeri Gunung Sugih Nomor 124/Pid.B/2025/PN Gns. Dalam perkara tersebut, terdakwa Almandela menggunakan akun media sosial untuk mengunggah video hasil manipulasi berbasis *artificial intelligence* yang mencatut Presiden Prabowo Subianto, seolah-olah menawarkan bantuan uang kepada masyarakat. Video tersebut disertai nomor WhatsApp yang mengarahkan korban untuk menghubungi pelaku dan melakukan pembayaran sejumlah uang dengan dalih biaya pendaftaran, administrasi, pajak, atau pencairan bantuan.[10]

Perkara tersebut menunjukkan bahwa *deepfake* dapat digunakan sebagai sarana untuk membentuk keyakinan palsu pada korban. Dalam putusan, perbuatan terdakwa tidak hanya dipandang sebagai penyebaran konten manipulatif, tetapi juga sebagai perbuatan yang berkaitan dengan manipulasi Informasi Elektronik dan/atau Dokumen Elektronik agar dianggap seolah-olah sebagai data yang otentik. Majelis hakim kemudian mempertimbangkan dakwaan Pasal

[9] Polri, "Tim Siber Ungkap Teknologi Deepfake Catut Nama Pejabat Negara."

[10] Humas Polda Maluku, "Dittipidsiber Tangkap Pelaku Deepfake Presiden Prabowo Dan Pejabat Negara Lainnya," Humas Polda Maluku, 2025, https://tribratanews.maluku.polri.go.id/informasi/berita/baca/dittipidsiber-tangkap-pelaku-deepfake-presiden-prabowo-dan-pejabat-negara-lainnya.

51 ayat (1) jo. Pasal 35 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Unsur yang dipertimbangkan meliputi unsur "setiap orang" serta unsur "dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, atau pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar dianggap seolah-olah data yang otentik".

Isu hukum dalam perkara ini menjadi penting karena *deepfake* belum diatur secara khusus sebagai delik tersendiri dalam hukum pidana Indonesia. Namun demikian, perbuatan penyalahgunaan *deepfake* tetap dapat dianalisis melalui ketentuan hukum pidana yang berlaku, terutama Kitab Undang-Undang Hukum Pidana (KUHP), UU ITE, dan UU PDP. Dengan demikian, perbuatan penyalahgunaan *deepfake* perlu dikaji berdasarkan terpenuhi atau tidaknya unsur tindak pidana dalam peraturan perundang-undangan, bukan semata-mata karena penggunaan teknologi digital dalam perbuatan tersebut.

Untuk menilai terpenuhi atau tidaknya unsur tindak pidana tersebut, terlebih dahulu perlu dipahami pola perbuatan atau modus operandi yang digunakan pelaku. Dalam perkara ini, modus operandi dilakukan dengan cara mengunggah video *deepfake* di media sosial yang seolah-olah berisi pengumuman bantuan sosial dari Presiden Prabowo Subianto[11]. Video tersebut kemudian disertai nomor WhatsApp yang mengarahkan calon korban untuk menghubungi pelaku. Setelah korban percaya terhadap isi video tersebut, pelaku meminta korban mengirimkan sejumlah uang dengan alasan biaya pendaftaran, administrasi, pajak, atau pencairan bantuan. Pola ini menunjukkan bahwa *deepfake* tidak hanya digunakan sebagai konten

[11] Tempo, "Polisi Ungkap Modus Penipuan Yang Gunakan Video Presiden Prabowo Subianto," *Tempo*, January 2025, https://www.tempo.co/arsip/polisi-ungkap-modus-penipuan-yang-gunakan-video-presiden-prabowo-subianto--1197972.

palsu, tetapi juga sebagai sarana untuk membangun kepercayaan korban dan memperoleh keuntungan secara melawan hukum.[12]

Penyalahgunaan *deepfake* dalam modus penipuan digital juga terlihat dalam pemberitaan Tribratanews Polri mengenai banyaknya korban penipuan bantuan sosial palsu. Penyelidikan Bareskrim menemukan bahwa pelaku berinisial JS di Lampung diduga memperoleh Rp65 juta dari sekitar 100 korban di 20 provinsi.[13] Kondisi ini menunjukkan bahwa *deepfake* tidak hanya menimbulkan persoalan teknis dalam membedakan konten asli dan palsu, tetapi juga menimbulkan persoalan hukum terkait kerugian korban, pembuktian digital, serta pertanggungjawaban pidana pelaku.[14] Oleh karena itu, penegakan hukum terhadap penyalahgunaan *deepfake* menjadi penting untuk memberikan perlindungan terhadap masyarakat dalam ruang digital.[15]

Berdasarkan hasil studi literatur yang telah dilakukan, perkembangan teknologi *AI* di era revolusi industri 4.0 telah menimbulkan tantangan serius terhadap sistem hukum di Indonesia. Teknologi seperti *deepfake* yang mampu merekayasa citra dan suara manusia secara realistis telah digunakan dalam berbagai tindak pidana

---

[12] Normatriya Sofiana Ana, Muhammad Purnomo, and Dian Rosita, "Analisi Yuridis Tindak Pidana Love Scamming Sebagai Tindak pidana digital," *Semarang Law Review (SLR)* 6, no. 2 (2025): 282–98, https://doi.org/https://doi.org/10.26623/slr.v6i2.12661.

[13] Tribratanews Polri, "Penyebar Deepfake Presiden Ditangkap, Sudah Raih Keuntungan Hingga Rp65 Juta" (Jakarta, 2025), https://tribratanews.polri.go.id/blog/hukum-4/penyebar-deepfake-presiden-ditangkap-sudah-raih-keuntungan-hingga-rp65-juta-83865.

[14] Hendra Prayoga and Hadi Tuasikal, "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia," *Abdurrauf Law and Sharia* 2, no. 1 (2025): 22–38, https://doi.org/https://doi.org/10.70742/arlash.v2i1.194.

[15] Yang Meliana, "Urgensi Formulasi Perlindungan Hukum Dan Kepastian Pidana Terhadap Pengaturan Tindak Pidana Deepfake Dalam Sistem Hukum Pidana Nasional," *Jurnal Hukum Lex Generalis* 6, no. 7 (2025), https://doi.org/https://doi.org/10.56370/jhlg.v6i7.1087.

digital. Penelitian yang dilakukan oleh Wahyudi Br[16] menunjukkan bahwa penegakan hukum terhadap tindak pidana berbasis AI masih menghadapi hambatan besar, salah satunya adalah kekosongan regulasi yang secara khusus mengatur teknologi tersebut, sehingga proses pertanggungjawaban hukum menjadi tidak optimal. Kebutuhan akan reformasi hukum juga disuarakan oleh Adnasohn Aqilla Respati[17], yang melalui kajiannya menyimpulkan bahwa UU ITE di Indonesia perlu direformulasi agar mampu menyesuaikan dengan perkembangan pesat *AI*, dengan merujuk pada regulasi *AI* yang diterapkan di Uni Eropa dan China. Penelitian ini juga menyoroti perlunya otoritas pengawasan khusus terhadap risiko pemanfaatan *AI*, terutama dalam konteks *deepfake*.

Selain itu, Nadea Aulia Putri and Maria Novita Apriyani[18] mengupas pertanggungjawaban pidana atas penggunaan *AI* dalam bentuk *deepfake* yang merugikan korban secara pribadi, sangat relevan dengan aspek pidana dan teknologi *AI*. Senada dengan itu, Penelitian oleh Yoan Shevila Kristiyenda, Jasmine Faradila and Christina Basanova[19] menganalisis modus kejahatan penipuan menggunakan *deepfake* tokoh pimpinan negara yaitu Prabowo Subianto, dan penelitian ini menekankan lemahnya regulasi serta perlunya

---

[16] Wahyudi Br, "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI," *Innovative: Journal of Social Science Research* 5, no. 1 (2025), https://doi.org/https://doi.org/10.31004/innovative.v5i1.17519.

[17] Adnasohn Aqilla Respati, "Reformulasi Undang-Undang ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation," *Jurnal USM LawReview* 7, no. 3 (2024): 4–12, https://doi.org/https://doi.org/10.26623/julr.v7i3.10578.

[18] Nadea Aulia Putri and Maria Novita Apriyani, "Pertanggungjawaban Pidana Pelaku Kekerasan Seksual Berbasis Elektronik Artificial Intelegence (Deep Fake Porn)," *Wajah Hukum* 9, no. 1 (2025): 348–58, https://doi.org/10.33087/wjh.v9i1.1725.

[19] 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. April (2025), https://doi.org/https://doi.org/10.59246/aladalah.v2i4.

penguatan kebijakan adaptif dan kolaborasi antara pemerintah dan *platform* digital. lebih menyoroti aspek perlindungan hukum korban *deepfake porn*, dengan pendekatan preventif melalui literasi digital serta normatif melalui perlindungan data pribadi berdasarkan UU ITE dan konsep "*Right to be Forgotten*". Sementara itu, penelitian dari Rizgita Nurul Fauzyah, Putri Hafidati and Sunarya Sunarya[20] membahas secara mendalam urgensi regulasi khusus terhadap penyalahgunaan *AI* dalam konteks pornografi palsu, serta pentingnya klasifikasi risiko dalam pemanfaatan *AI* untuk perlindungan hukum yang efektif. Kelima penelitian ini menunjukkan adanya keseragaman urgensi terhadap penyusunan regulasi hukum yang adaptif dalam menghadapi tindak pidana digital berbasis *AI* termasuk *deepfake* yang secara langsung berkaitan dengan isu tanggung jawab pidana dan perlindungan korban di Indonesia terhadap penyalahgunaan *AI*.

Mengacu pada penelitian-penelitian sebelumnya, penelitian ini memiliki kesamaan tema dalam mengkaji isu hukum terkait penyalahgunaan teknologi digital, khususnya *deepfake*. Namun, kebaruan penelitian ini terletak pada fokus analisis yang menempatkan *deepfake* sebagai bentuk penyalahgunaan teknologi AI dalam modus penipuan digital, bukan sekadar sebagai video editan yang menyerupai Presiden. Dengan demikian, penelitian ini diarahkan untuk melihat bagaimana *deepfake* digunakan sebagai sarana memperdaya korban, membentuk keyakinan palsu, dan menimbulkan persoalan hukum dalam aspek pembuktian digital, pertanggungjawaban pidana, serta penyalahgunaan identitas digital berupa wajah dan suara.

Berdasarkan kebaruan tersebut, penelitian ini bertujuan menganalisis pemenuhan unsur tindak pidana dalam penyalahgunaan

---

[20] Rizgita Nurul Fauzyah, Putri Hafidati, and Sunarya Sunarya, "Perlindungan Hukum Terhadap Korban Tindak Pidana Pembuat Video Pornografi Palsu (Deepfake Porn) Berbasis Artificial Intelligence (AI) Di Indonesia," *Lex Veritatis* 3, no. November (2024): 74–88, https://ejournal.unis.ac.id/index.php/JournalMahasiswa/article/download/5140/2549.

deepfake melalui ketentuan KUHP dan UU ITE, serta menilai pertanggungjawaban pidana pelaku berdasarkan asas legalitas atau *nullum crimen sine lege*. Selain itu, UU PDP juga digunakan sebagai instrumen normatif pendukung untuk menilai penyalahgunaan identitas digital berupa wajah dan suara yang dimanipulasi melalui teknologi *deepfake*. Oleh karena itu, pertanyaan dalam penelitian ini adalah:

1. Bagaimana modus operandi penyalahgunaan teknologi deepfake *artificial intelligence* di Indonesia?
2. Bagaimana tanggung jawab hukum penyalahgunaan teknologi deepfake *artificial intelligence* di Indonesia?

Untuk menjawab pertanyaan penelitian, teori pertanggungjawaban pidana digunakan sebagai kerangka teori dalam menganalisis penyalahgunaan teknologi AI, khususnya *deepfake*, dalam tindak pidana penipuan digital. Penelitian ini berfokus pada pemenuhan unsur tindak pidana dan pertanggungjawaban pidana pelaku. Dalam Kitab Undang-Undang Hukum Pidana, pertanggungjawaban pidana tidak hanya dilihat dari terpenuhinya perbuatan pidana, tetapi juga dari adanya unsur kesalahan pelaku, kemampuan bertanggung jawab, serta tidak adanya alasan pembenar maupun alasan pemaaf. Oleh karena itu, penggunaan *deepfake* dalam modus penipuan digital dianalisis melalui perbuatan pelaku dalam membuat dan menyebarkan informasi elektronik yang dimanipulasi, adanya kesengajaan untuk memperdaya korban, serta dapat atau tidaknya pelaku dimintai pertanggungjawaban pidana.

Mengingat kecerdasan buatan (*AI*) masih menjadi hal baru yang terus berkembang di Indonesia, penelitian ini diharapkan dapat memberikan kontribusi akademik dalam pengembangan kajian hukum pidana terhadap penyalahgunaan teknologi AI, khususnya *deepfake*, serta memberikan kontribusi praktis dalam merumuskan pertanggungjawaban pidana terhadap pelaku tindak pidana digital berbasis AI. Namun, limitasi penelitian ini yaitu hanya terbatas pada

pengkajian aspek hukum yang berlaku di Indonesia. Sehingga membatasi generalisasi akademik yang bersumber dari regulasi Internasional.

Metode Penelitian

Penelitian hukum ini adalah menggunakan metode penelitian hukum normatif.[21] Karakteristik tujuan penelitian ini adalah untuk melakukan analisis terhadap ketaatan masyarakat terhadap hukum, serta implikasi dari ketaatan atau pelanggaran terhadap stabilitas hukum dan penerapan keadilan.[22]

Pendekatan penelitian yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan, pendekatan kasus, dan pendekatan konseptual.[23] Pendekatan perundang-undangan digunakan untuk mengkaji norma-norma hukum yang relevan, seperti Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Pendekatan kasus digunakan untuk menelaah putusan pengadilan negeri Gunung Sugih Nomor 124/Pid.B/2025/PN Gns mengenai tindak pidana manipulasi informasi elektronik melalui video deepfake yang mencatut Presiden

---

[21] Hari Sutra Disemadi, "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies," *Journal of Judicial Review* 24, no. 2 (2022): 289, https://doi.org/10.37253/jjr.v24i2.7280.

[22] David Tan, "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum," *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 8, no. 5 (2021): 1332–36.

[23] Muhamad Azhar Kornelius Benuf, "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Staf Badan Konsultasi Hukum, Fakultas Hukum Universitas Diponegoro* 7, no. 1 (2020): 1–14, https://www.scribd.com/document/511815132/Jurnal-MPH-Metodologi-Penelitian-Hukum-Sebagai-Instrumen-Mengurai-Permasalahan-Hukum-Kontemporer?

Prabowo Subianto dalam skema penipuan bantuan. Pendekatan konseptual digunakan untuk menggali konsep pertanggungjawaban hukum atas penyalahgunaan teknologi kecerdasan buatan dan relevansinya dengan asas legalitas. Bahan hukum dalam penelitian ini terdiri atas bahan hukum primer dan bahan hukum sekunder,[24] bahan hukum primer yaitu peraturan perundang-udangan, KUHP, UU ITE dan UU PDP. Adapun bahan hukum sekunder berupa literatur, buku, jurnal, artikel ilmiah, dan karya tulis ilmiah. Bahan-bahan hukum ini diperoleh melalui studi kepustakaan dan dianalisis melalui secara deskriptif menggunakan teknik interpretasi hukum untuk memperoleh kesimpulan yang benar.[25]

Teori pertanggungjawaban pidana digunakan sebagai alat analisis untuk menilai penyalahgunaan teknologi AI, khususnya *deepfake*, dalam tindak pidana penipuan digital. Analisis diarahkan pada terpenuhinya unsur kejahatan dan pelanggaran, unsur kesalahan pelaku, kemampuan bertanggung jawab, serta ada atau tidaknya alasan pembenar maupun alasan pemaaf. Dalam perkara ini, analisis didasarkan pada UU ITE sebagai dasar pemidanaan utama, KUHP lama sebagai dakwaan alternatif mengenai penipuan, dan UU PDP sebagai dasar normatif pendukung terkait penyalahgunaan identitas digital berupa wajah dan suara.

Hasil dan Pembahasan

A. Modus Operandi Penyalahgunaan Teknologi *Deepfake Artificial Intelligence* di Indonesia

Seiring dengan pesatnya perkembangan teknologi, hadirnya kecerdasan buatan atau *Artificial Intelligence* (*AI*) telah membuka

[24] Hari Sutra Disemadi, "Lensa Penelitian Hukum: Esai Deskriptif Tentang Metodologi Penelitian Hukum," *Journal of Judicial Review* 24, no. 2 (2022): 289, https://doi.org/10.37253/jjr.v24i2.7280.

[25] Tan, "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum."

berbagai peluang baru di berbagai sektor, termasuk dalam dunia digital.[26] Salah satu aplikasi AI yang semakin berkembang dan menarik perhatian adalah teknologi *deepfake*, yang memungkinkan manipulasi gambar, video, atau suara secara realistis dengan menggunakan algoritma canggih.[27] Penggunaan teknologi ini, meskipun memiliki potensi positif, telah menimbulkan kekhawatiran serius terkait dampaknya terhadap privasi, keamanan, dan reputasi individu, serta potensi penyalahgunaannya untuk kepentingan pribadi atau kelompok tertentu. Fenomena penyalahgunaan *deepfake* menjadi isu yang mendesak, terutama dalam kaitannya dengan penipuan, pencemaran nama baik, dan tindak pidana lainnya. Oleh karena itu, penting bagi kerangka hukum Indonesia untuk mengadopsi pendekatan yang komprehensif, yang tidak hanya bersifat reaktif, namun juga proaktif dalam menangani potensi risiko yang ditimbulkan oleh penyalahgunaan teknologi ini.

Modus operandi merujuk pada pola atau cara khas yang digunakan oleh pelaku tindak pidana untuk melaksanakan tindakannya.[28] Istilah ini berasal dari bahasa Latin yang secara harfiah berarti "cara beroperasi" dan sering kali digunakan untuk menggambarkan metode tertentu yang menjadi ciri khas dari setiap pelaku dalam melakukan tindak pidana.[29] Pemahaman terhadap

---

[26] Gabriella Patricia Setyawan, Fendy Fendy, and Kamaluddin Mantasa, "Perpustakaan Di Era Digital: Menjaga Eksistensi Di Tengah Dominasi Kecerdasan Buatan (Artificial Intelligence)," *Journal Papyrus: Sosial, Humaniora, Perpustakaan Dan Informasi* 4, no. 1 (2025): 49–58, https://doi.org/https://doi.org/10.59638/jp.v4i1.82.

[27] Yoggy Arif Fernandes and Yulia Fatma, "Metode Deep Learning Dalam Teknologi Deepfake: Systematic Literature Review," *JATI (Jurnal Mahasiswa Teknik Informatika)* 9, no. 2 (2025): 3403–10, https://mail.ejournal.itn.ac.id/index.php/jati/article/view/12987.

[28] Andre Herdian and Untung Sumarwan, "Analisis Kriminologi Deepfake Melalui Media Sosial Berdasarkan Teori Rational Choice," *IKRA-ITH HUMANIORA: Jurnal Sosial Dan Humaniora* 9, no. 1 (2025): 323–31, https://doi.org/10.37817/ikraith-humaniora.

[29] Alaq Thariq Takarianta, "Penegakan Hukum Terhadap Pencurian Ikan Oleh Kapal Asing Di Perairan Indonesia," *LEX PRIVATUM* 14, no. 5

modus operandi sangat penting dalam analisis kriminal, karena dapat memberikan petunjuk mengenai motif, karakteristik, serta taktik yang digunakan oleh pelaku, yang pada gilirannya dapat membantu dalam proses penyelidikan dan penanganan kasus. Dalam tindak pidana digital, modus operandi bisa melibatkan penggunaan berbagai teknologi canggih untuk menipu, memanipulasi, atau merusak reputasi seseorang atau institusi, seperti yang dapat terjadi pada kasus-kasus penyalahgunaan teknologi *deepfake*.[30]

Dalam hukum pidana Indonesia, suatu perbuatan dapat dimintakan pertanggungjawaban pidana apabila memenuhi unsur-unsur tindak pidana yang dirumuskan dalam peraturan perundang-undangan. Modus operandi pelaku perlu dilihat dari dua aspek. Pertama, apakah perbuatan tersebut memenuhi unsur-unsur tindak pidana berdasarkan ketentuan hukum yang berlaku, khususnya KUHP, UU ITE. Kedua, apakah penggunaan teknologi *deepfake* menimbulkan kompleksitas hukum dalam pembuktian, terutama karena karakter teknologi tersebut mampu memanipulasi wajah, suara, dan informasi elektronik sehingga sulit dibedakan dari data yang otentik. Dalam perkara penyalahgunaan *deepfake*, pola tersebut dapat terlihat dari tindakan pelaku membuat atau menyebarkan konten manipulatif, mencatut wajah dan suara tokoh publik, mencantumkan nomor kontak, serta meminta sejumlah uang dengan alasan tertentu. Dengan demikian, modus operandi penyalahgunaan *deepfake* tidak hanya dipahami sebagai cara pelaku menyebarkan video palsu, tetapi juga sebagai pola penipuan digital yang berkaitan dengan manipulasi identitas digital, pembuktian elektronik, dan pemenuhan unsur tindak pidana.

Dalam Putusan Pengadilan Negeri Gunung Sugih Nomor 124/Pid.B/2025/PN Gns, modus operandi penyalahgunaan *deepfake*

(2025), https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/60238.

[30] Prayoga and Tuasikal, "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia."

terlihat dari tindakan terdakwa Almandela yang menggunakan akun media sosial untuk mengunggah video hasil manipulasi berbasis AI dengan mencatut Presiden Prabowo Subianto seolah-olah menawarkan bantuan uang kepada masyarakat. Video tersebut disertai nomor WhatsApp yang mengarahkan calon korban untuk menghubungi terdakwa. Setelah korban percaya terhadap isi video tersebut, terdakwa meminta sejumlah uang dengan alasan biaya pendaftaran, administrasi, pajak, atau pencairan bantuan.

Pola tersebut menunjukkan bahwa *deepfake* dalam perkara ini tidak hanya berfungsi sebagai video editan, tetapi sebagai instrumen penipuan digital. Citra dan suara tokoh publik digunakan untuk menciptakan kesan seolah-olah informasi dalam video tersebut benar dan berasal dari pihak yang berwenang. Dengan demikian, kebaruan modus dalam perkara ini terletak pada penggunaan teknologi AI untuk memanipulasi identitas digital berupa wajah dan suara, sehingga korban terdorong untuk mempercayai informasi palsu dan menyerahkan uang kepada pelaku.

Secara yuridis, modus tersebut berkaitan dengan Pasal 51 ayat (1) jo. Pasal 35 UU ITE, yaitu perbuatan dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, atau pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar dianggap seolah-olah sebagai data yang otentik. Dengan kata lain, niat terdakwa agar video terlihat asli ke publik mencakup unsur manipulasi informasi elektronik. Selanjutnya, penyebaran video yang mengelabui korban dan mengarahkan mereka untuk membayar uang masuk ke dalam konstruksi penipuan. Pasal 378 KUHP mensyaratkan adanya "tipu muslihat atau rangkaian kata bohong" yang menggerakkan korban menyerahkan uang. Pada kasus ini, *tipu muslihat*-nya terletak pada konten video palsu dan narasi fiktif bantuan yang mengelabui korban, sedangkan permintaan transfer uang merupakan tindakan "menggerakkan korban menyerahkan uang". Dengan demikian, unsur penipuan terpenuhi pada tahap korban mentransfer uang berdasarkan informasi bohong.

Sementara itu, UU PDP turut menggambarkan konteks penyalahgunaan identitas digital. Misalnya, UU PDP Pasal 65 melarang "membuat data pribadi palsu atau memalsukan data pribadi" untuk keuntungan sendiri yang merugikan orang lain. Meskipun UU PDP tidak digunakan sebagai dasar pemidanaan dalam putusan ini, norma tersebut tetap memiliki relevansi dalam membaca dimensi penyalahgunaan identitas digital, sebab manipulasi wajah dan suara seseorang melalui teknologi *deepfake* dapat dikaitkan dengan larangan pemalsuan atau penyalahgunaan data pribadi yang berpotensi merugikan subjek data.

Berdasarkan uraian tersebut, modus operandi penyalahgunaan *deepfake* dalam perkara ini dapat dipahami melalui beberapa tahapan. Pertama, pelaku menggunakan atau memanfaatkan video hasil manipulasi berbasis AI. Kedua, pelaku mencatut identitas tokoh publik untuk membangun kepercayaan masyarakat. Ketiga, pelaku menyebarkan video tersebut melalui media sosial dan mencantumkan nomor WhatsApp sebagai sarana komunikasi. Keempat, pelaku meminta korban mengirimkan sejumlah uang dengan alasan biaya administrasi, pajak, atau pencairan bantuan. Tahapan ini menunjukkan bahwa penyalahgunaan *deepfake* dalam penipuan digital bekerja melalui kombinasi antara manipulasi teknologi, penyalahgunaan identitas digital, dan tipu muslihat terhadap korban.

Namun, salah satu tantangan utama dalam penegakan hukum terhadap tindak pidana berbasis *deepfake* di Indonesia adalah belum adanya pengaturan khusus mengenai *deepfake*, kerentanan alat bukti elektronik terhadap manipulasi, serta keterbatasan kapasitas forensik digital aparat penegak hukum.[31] Bukti berupa video atau gambar palsu sering kali sulit dilacak keasliannya, terlebih apabila pelaku menggunakan teknologi untuk menghapus atau menyamarkan jejak

[31] Dwi Fitri et al., "Deepfake Dan Krisis Kepercayaan: Analisis Hukum Terhadap Penyebaran Konten Palsu Di Media Sosial," *Jurnal Intelek Insan Cendikia* 2, no. 6 (2025): 11556–68, https://jicnusantara.com/index.php/jiic.

digital.[32] Oleh karena itu, pendekatan pembuktian digital yang adaptif diperlukan, khususnya melalui penguatan forensik digital, autentikasi konten elektronik, dan pelacakan jejak digital dalam proses peradilan pidana.[33]

B. Tanggung Jawab Hukum Penyalahgunaan Teknologi *Deepfake Artificial Intelligence* di Indonesia

Istilah tanggung jawab hukum difokuskan secara khusus pada pertanggungjawaban pidana pelaku penyalahgunaan teknologi *deepfake* berdasarkan konsep hukum pidana. Dalam hukum pidana, pertanggungjawaban pidana mensyaratkan adanya unsur tindak pidana, kesalahan (sengaja/kealpaan), kemampuan pelaku untuk bertanggung jawab, serta tidak adanya alasan pembenar atau pemaaf. Analisis pertanggungjawaban terhadap penyalahgunaan *deepfake* tidak cukup menyoroti teknologi AI-nya semata, melainkan harus memeriksa apakah pelaku memenuhi semua unsur tersebut berdasarkan KUHP dan UU ITE. Oleh karena itu, penilaian pertanggungjawaban pidana pelaku harus dilihat dari kesadaran pelaku menggunakan manipulasi *deepfake* tersebut untuk memperdaya korban dan memperoleh keuntungan, sehingga unsur kesengajaan dan tipu muslihat terpenuhi.

Menurut KUHP, seseorang hanya dapat dipidana jika telah memenuhi unsur tindak pidana dan sengaja atau alpa melakukan

---

[32] Yang Meliana, "Urgensi Formulasi Perlindungan Hukum Dan Kepastian Pidana Terhadap Pengaturan Tindak Pidana Deepfake Dalam Sistem HukumPidana Nasional (The Urgency Of Formulating Legal Protection and Criminal Law Certainty Regarding The Regulation Of Deepfake Crimes With," *Rewang Rencang: Jurnal Hukum Lex Generalis* 6, no. 7 (2025): 1–12, https://publikasi.rewangrencang.com/.

[33] B R Wahyudi, "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI," *INNOVATIVE: Journal Of Social Science Research* 5, no. 1 (2025): 3436–50, https://doi.org/https://doi.org/10.31004/innovative.v5i1.17519.

perbuatan tersebut. Elemen utama pertanggungjawaban pidana mencakup, 1. Perbuatan pidana: Ada perbuatan materiil yang melanggar hukum (misalnya manipulasi informasi elektronik), 2. Kesalahan (*schuld*): Pelaku mengetahui dan menghendaki perbuatannya (kesengajaan) atau setidaknya lalai (kealpaan) melakukan perbuatan itu, 3. Kemampuan bertanggung jawab: Pelaku mentalnya sehat sehingga mampu menyadari perbuatan dan akibatnya (Pasal 44 KUHP), 4. Tiada alasan pembenar/pemaaf: Tidak ada kondisi seperti terpaksa, perintah sah, atau keadaan darurat yang membebaskan hukuman (Pasal 48–51 KUHP).

Jika salah satu unsur ini tidak terpenuhi, pertanggungjawaban pidana gugur. Dalam perkara ini, fakta bahwa terdakwa menggunakan teknologi *deepfake* untuk melakukan penipuan menunjukkan ia tidak dalam keadaan terpaksa atau tidak sadar, sehingga kondisi pembelaan terpaksa (*noodweer*) maupun daya paksa (*overmacht*) tidak relevan. Tidak ada indikasi gangguan jiwa atau ketidakmampuan mental, sehingga Pasal 44 KUHP tidak dapat diterapkan. Dengan demikian, pelaku dapat dinilai mampu bertanggung jawab sepenuhnya atas perbuatannya.

Dalam Putusan PN Gunung Sugih 124/Pid.B/2025, majelis hakim menilai bahwa perbuatan terdakwa mencakup pembuatan dan penyebaran video deepfake yang mencatut Presiden Prabowo Subianto serta permintaan uang kepada korban melalui tipu muslihat. Dari sudut hukum pidana, perbuatan ini dikualifikasikan sebagai manipulasi Informasi Elektronik (Pasal 35 UU ITE) dengan tujuan menipu (Pasal 378 KUHP). Keberadaan unsur objek (informasi elektronik palsu) dan subjek (pelaku) sudah nyata. Yang menjadi perhatian adalah unsur kesengajaan: terdakwa tidak sekadar tidak sengaja mengubah wajah dalam video, tetapi melakukan aksi tersebut sengaja untuk membangun keyakinan palsu korban dan menguntungkan diri sendiri. Fakta-fakta seperti pencantuman nomor WhatsApp pribadi dan permintaan uang menguatkan adanya niat jahat (*mens rea*) pelaku. Dengan kata lain, pelaku tahu bahwa video itu

tidak otentik namun tetap menyebarkannya untuk menipu. Ini memenuhi unsur kesengajaan dalam tindak pidana penipuan.

Dalam perumusan delik, yang menjadi inti pertanggungjawaban bukan sekadar pemanfaatan teknologi AI, melainkan tindakan sadar pelaku yang menggunakan video palsu tersebut sebagai alat kejahatan. Pasal 51 ayat (1) jo. Pasal 35 UU ITE mensyaratkan adanya perbuatan melawan hukum dengan memanipulasi informasi elektronik agar tampak otentik. Kasus *deepfake* ini jelas masuk kategori tersebut, karena terdakwa dengan sengaja menggunakan wajah Presiden untuk membuat informasi elektronik menyesatkan. Dengan demikian, inti pertanggungjawaban pidana bukan terletak pada penggunaan teknologi AI semata, melainkan pada tindakan sadar pelaku yang memanfaatkan teknologi tersebut untuk memanipulasi informasi elektronik dan memperdaya korban.

KUHP menegaskan bahwa pelaku tidak dipidana jika tidak mampu bertanggung jawab (Pasal 44 KUHP). Dalam perkara ini, tidak ada bukti bahwa terdakwa menderita gangguan jiwa atau ketidakmampuan mental. Sebaliknya, perbuatan terdakwa terorganisir dari manipulasi video hingga komunikasi dengan korban menunjukkan kontrol dan pemahaman penuh terhadap tindakannya. Oleh karena itu, unsur kemampuan bertanggung jawab terpenuhi. Selain itu, KUHP (Pasal 48–51) menyebut alasan-alasan yang dapat menghapus pidana, seperti tekanan luar biasa (*overmacht*), pembelaan terpaksa (*noodweer*), melaksanakan undang-undang, atau perintah jabatan. Fakta kasus tidak menunjukkan kondisi-kondisi tersebut. Terdakwa tidak berada di bawah ancaman mematikan, tidak membela diri dari serangan, dan tidak bertindak atas perintah resmi. Semua tahap aksi dilakukan atas inisiatif sendiri, sehingga tidak terdapat alasan pembenar/pemaaf yang dapat membebaskannya dari pertanggungjawaban.

Prinsip legalitas (*nullum crimen sine lege*) mensyaratkan bahwa suatu tindakan baru dapat dipidana apabila telah diatur dalam peraturan perundang-undangan sebelum perbuatan dilakukan. Kasus deepfake

ini menjadi ilustrasi penting, meskipun *deepfake* sebagai istilah teknologi tidak disebutkan secara eksplisit dalam KUHP atau UU ITE, perbuatan terdakwa dapat dikualifikasikan berdasarkan norma yang sudah ada. Hakim dalam putusan tersebut menerapkan Pasal 35 jo. Pasal 51 UU ITE sebagai hukum khusus (lex specialis) atas manipulasi informasi elektronik, dengan Pasal 378 KUHP sebagai dakwaan alternatif untuk unsur penipuan. Hal ini sesuai asas legalitas karena tidak menambah delik baru, tetapi menempatkan tindakan pelaku dalam kategori penipuan digital. UU ITE berperan sebagai basis utama yakni mengubah informasi elektronik palsu agar dianggap asli, sementara KUHP menggarisbawahi unsur membohongi korban untuk keuntungan pribadi. Dengan demikian, pelaku tidak dihukum karena menggunakan AI, melainkan karena memenuhi kualifikasi tipu muslihat dalam tindak pidana penipuan dan manipulasi data elektronik.

Walaupun UU PDP tidak menjadi dasar hukum pidana dalam putusan ini, UU PDP memperkaya analisis terkait *deepfake* sebagai penyalahgunaan identitas digital. *Deepfake* identik dengan memanipulasi data biometrik wajah, suara, dan fitur pribadi seseorang tanpa izin. Dalam perspektif UU PDP, tindakan ini melanggar hak perlindungan data pribadi individu. Sebagaimana dicatat penelitian, penggunaan wajah/suara tanpa izin dapat melanggar hak individu atas data pribadinya dan "memanipulasi citra atau suara seseorang tanpa izin jelas merupakan pelanggaran terhadap hak individu" sebagaimana diatur Pasal 4 dan 9 UU PDP. UU PDP menegaskan setiap pengumpulan/pengolahan data pribadi harus dengan persetujuan pemilik data, sehingga tindakan *deepfake* yang mengambil dan memalsukan identitas pribadi tanpa izin menjadi pelanggaran terhadap asas tersebut. Dalam pembahasan ini, UU PDP hanya dipakai untuk menyoroti dimensi penyalahgunaan identitas yang tidak dibahas dalam KUHP/ITE, misalnya merugikan reputasi atau privasi korban. Dengan demikian, UU PDP tidak menggantikan basis pemidanaan UU ITE/KUHP, tetapi menegaskan bahwa wajah dan suara digital juga layak dilindungi.

Dengan demikian, persoalan utama dalam pertanggungjawaban pidana penyalahgunaan *deepfake* bukan semata-mata ketiadaan delik khusus bernama *deepfake*, melainkan bagaimana hukum pidana mengualifikasikan perbuatan pelaku berdasarkan unsur tindak pidana yang telah ada. Dalam perkara ini, penggunaan *deepfake* berfungsi sebagai sarana untuk melakukan manipulasi informasi elektronik dan memperkuat tipu muslihat dalam penipuan digital. Oleh karena itu, pelaku tetap dapat dimintai pertanggungjawaban pidana sepanjang dapat dibuktikan adanya perbuatan, kesalahan, kemampuan bertanggung jawab, dan tidak adanya alasan penghapus pidana.

Kesimpulan

Berdasarkan pembahasan yang telah diuraikan, dapat disimpulkan bahwa modus operandi penyalahgunaan teknologi *deepfake artificial intelligence* dalam Putusan Pengadilan Negeri Gunung Sugih Nomor 124/Pid.B/2025/PN Gns dilakukan melalui pemanfaatan video hasil manipulasi berbasis AI yang mencatut Presiden Prabowo Subianto seolah-olah menawarkan bantuan uang kepada masyarakat. Video tersebut disebarkan melalui media sosial dan disertai nomor WhatsApp untuk mengarahkan korban berkomunikasi dengan pelaku. Setelah korban percaya, pelaku meminta sejumlah uang dengan alasan biaya pendaftaran, administrasi, pajak, atau pencairan bantuan. Pola tersebut menunjukkan bahwa *deepfake* tidak hanya digunakan sebagai konten palsu, tetapi juga sebagai sarana untuk membangun keyakinan palsu, memanipulasi identitas digital, dan memperkuat tipu muslihat dalam tindak pidana penipuan digital.

Tanggung jawab hukum dalam penyalahgunaan teknologi *deepfake artificial intelligence* pada perkara ini pada dasarnya merupakan pertanggungjawaban pidana. Pelaku dapat dimintai pertanggungjawaban karena perbuatannya memenuhi unsur tindak pidana, terdapat kesalahan dalam bentuk kesengajaan, pelaku memiliki kemampuan bertanggung jawab, serta tidak ditemukan

alasan pembenar maupun alasan pemaaf. Pertanggungjawaban pidana tersebut didasarkan pada Pasal 51 ayat (1) jo. Pasal 35 UU ITE sebagai dasar utama mengenai manipulasi Informasi Elektronik dan/atau Dokumen Elektronik agar dianggap seolah-olah sebagai data yang otentik, serta Pasal 378 KUHP sebagai dakwaan alternatif mengenai penipuan. Adapun UU PDP tidak menjadi dasar pemidanaan dalam putusan, melainkan sebagai instrumen normatif pendukung untuk melihat dimensi penyalahgunaan identitas digital berupa wajah dan suara. Oleh karena itu, diperlukan penguatan pengaturan hukum, kapasitas pembuktian digital, dan harmonisasi antara KUHP, UU ITE, dan UU PDP agar penegakan hukum terhadap penyalahgunaan *deepfake* tidak hanya berorientasi pada kerugian ekonomi korban, tetapi juga memperhatikan perlindungan identitas digital pihak yang dimanipulasi.

Referensi

Journal

Ana, Normatriya Sofiana, Muhammad Purnomo, and Dian Rosita. "Analisi Yuridis Tindak Pidana Love Scamming Sebagai Tindak pidana digital." *Semarang Law Review (SLR)* 6, no. 2 (2025): 282–98. https://doi.org/https://doi.org/10.26623/slr.v6i2.12661.

Br, Wahyudi. "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI." *Innovative: Journal of Social Science Research* 5, no. 1 (2025). https://doi.org/https://doi.org/10.31004/innovative.v5i1.17519.

Disemadi, Hari Sutra. "Lensa Penelitian Hukum: Esai Deskriptif Tentang Metodologi Penelitian Hukum." *Journal of Judicial Review* 24, no. 2 (2022): 289. https://doi.org/10.37253/jjr.v24i2.7280.

——. "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies." *Journal of Judicial Review* 24, no. 2 (2022): 289. https://doi.org/10.37253/jjr.v24i2.7280.

Fauzyah, Rizgita Nurul, Putri Hafidati, and Sunarya Sunarya. "Perlindungan Hukum Terhadap Korban Tindak Pidana Pembuat Video Pornografi Palsu (Deepfake Porn) Berbasis Artificial Intelligence (AI) Di Indonesia." *Lex Veritatis* 3, no.

November (2024): 74–88. https://ejournal.unis.ac.id/index.php/JournalMahasiswa/article/download/5140/2549.

Fernandes, Yoggy Arif, and Yulia Fatma. "Metode Deep Learning Dalam Teknologi Deepfake: Systematic Literature Review." *JATI (Jurnal Mahasiswa Teknik Informatika)* 9, no. 2 (2025): 3403–10. https://mail.ejournal.itn.ac.id/index.php/jati/article/view/12987.

Fitri, Dwi, Syakban Akbar, Nawal Mufidah, Rezita Ardhani Manurung, Dara Akila, Sania Izzati Ramadhani, Nazwa Hanifah Tanjung, Aulia Putri, Ade Nur Hidayah, and Muhammad Zikri. "Deepfake Dan Krisis Kepercayaan: Analisis Hukum Terhadap Penyebaran Konten Palsu Di Media Sosial." *Jurnal Intelek Insan Cendikia* 2, no. 6 (2025): 11556–68. https://jicnusantara.com/index.php/jiic.

Herdian, Andre, and Untung Sumarwan. "Analisis Kriminologi Deepfake Melalui Media Sosial Berdasarkan Teori Rational Choice." *IKRA-ITH HUMANIORA: Jurnal Sosial Dan Humaniora* 9, no. 1 (2025): 323–31. https://doi.org/10.37817/ikraith-humaniora.

Hernawan, Cleophila Nathania Putri, Debby Telly Antow, and Arie Sendow. "Tinjauan Hukum Mengenai Penyalahgunaan Artificial Intellingence Dalam Tindak Pidana Kekerasan Seksual." *Lex Privatum Jurnal Fakultas Hukum Unsrat* 15, no. 4 (2025): 12. https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/61860.

Judijanto, Loso. "Hukum Pidana Dan Tindak pidana digital:: Menanggulangi Ancaman Kejahatan Digital Di Era Teknologi." *Indonesian Research Journal on Education* 5, no. 1 (2025): 968–72. https://doi.org/https://doi.org/10.31004/irje.v5i1.2114.

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. April (2025). https://doi.org/https://doi.org/10.59246/aladalah.v2i4.

Mahadipta, Ngurah Gede Dwi, and I Made Windu Aditya. "Mendorong Inovasi: Peran Artificial Intelligence Dalam Akselerasi Industri Kreatif." *Jurnal Imagine* 4, no. 1 (2024): 1–6.

https://jurnal.idbbali.ac.id/index.php/imagine/article/view/1049.

Meliana, Yang. "Urgensi Formulasi Perlindungan Hukum Dan Kepastian Pidana Terhadap Pengaturan Tindak Pidana Deepfake Dalam Sistem Hukum Pidana Nasional." *Jurnal Hukum Lex Generalis* 6, no. 7 (2025). https://doi.org/https://doi.org/10.56370/jhlg.v6i7.1087.

Mutmainnah, Anti, Awalia Marwah Suhandi, and Yusuf Tri Herlambang. "Problematika Teknologi Deepfake Sebagai Masa Depan Hoax Yang Semakin Meningkat: Solusi Strategis Ditinjau Dari Literasi Digital." *UPGRADE: Jurnal Pendidikan Teknologi Informasi* 1, no. 2 (2024): 67–72. https://doi.org/https://doi.org/10.30812/upgrade.v1i2.3702.

Prayoga, Hendra, and Hadi Tuasikal. "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia." *Abdurrauf Law and Sharia* 2, no. 1 (2025): 22–38. https://doi.org/https://doi.org/10.70742/arlash.v2i1.194.

Putri, Nadea Aulia, and Maria Novita Apriyani. "Pertanggungjawaban Pidana Pelaku Kekerasan Seksual Berbasis Elektronik Artificial Intelegence (Deep Fake Porn)." *Wajah Hukum* 9, no. 1 (2025): 348–58. https://doi.org/10.33087/wjh.v9i1.1725.

Respati, Adnasohn Aqilla. "Reformulasi Undang-Undang ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation." *Jurnal USM LawReview* 7, no. 3 (2024): 4–12. https://doi.org/https://doi.org/10.26623/julr.v7i3.10578.

Setyawan, Gabriella Patricia, Fendy Fendy, and Kamaluddin Mantasa. "Perpustakaan Di Era Digital: Menjaga Eksistensi Di Tengah Dominasi Kecerdasan Buatan (Artificial Intelligence)." *Journal Papyrus: Sosial, Humaniora, Perpustakaan Dan Informasi* 4, no. 1 (2025): 49–58. https://doi.org/https://doi.org/10.59638/jp.v4i1.82.

Syaputra, Rendi. "Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artificial Inteligence (AI) Dari Perspektif Hukum Pidana Indonesia." *Jurnal Hukum Respublica*, 2024, 1–13. https://doi.org/https://doi.org/10.31849/respublica.v24i01.23327.

Takarianta, Alaq Thariq. "Penegakan Hukum Terhadap Pencurian Ikan Oleh Kapal Asing Di Perairan Indonesia." *LEX PRIVATUM* 14, no. 5 (2025). https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/60238.

Tan, David. "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum." *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 8, no. 5 (2021): 1332–36.

Wahyudi, B R. "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI." *INNOVATIVE: Journal Of Social Science Research* 5, no. 1 (2025): 3436–50. https://doi.org/https://doi.org/10.31004/innovative.v5i1.17519.

Yang Meliana. "Urgensi Formulasi Perlindungan Hukum Dan Kepastian Pidana Terhadap Pengaturan Tindak Pidana Deepfake Dalam Sistem HukumPidana Nasional (The Urgency Of Formulating Legal Protection and Criminal Law Certainty Regarding The Regulation Of Deepfake Crimes With." *Rewang Rencang: Jurnal Hukum Lex Generalis* 6, no. 7 (2025): 1–12. https://publikasi.rewangrencang.com/.

Website

Astuti, Nanin Koeswidi. "Pertanggungjawaban Pidana Pelaku Manipulasi Gambar, Suara Dan Vidio (Deepfake) Menurut Hukum Telematika Di Indonesia." *Universitas Kristen Indonesia*, 2025. http://repository.uki.ac.id/18421/1/PERTANGGUNGJAWABANPIDANAPELAKUMANIPULASIGAMBAR.pdf.

Garuda. "Data Pengguna AI Di Indonesia Update Terbaru," 2025. https://www.garuda.website/blog/data-pengguna-ai-indonesia/.

GoodStats. "10 Negara Pengguna AI Terbanyak, Indonesia Salah Satunya." GoodStats, 2024. https://data.goodstats.id/statistic/10-negara-pengguna-ai-terbanyak-indonesia-salah-satunya-RLlmC.

Humas Polda Maluku. "Dittipidsiber Tangkap Pelaku Deepfake Presiden Prabowo Dan Pejabat Negara Lainnya." Humas Polda Maluku, 2025.

https://tribratanews.maluku.polri.go.id/informasi/berita/baca/dittipidsiber-tangkap-pelaku-deepfake-presiden-prabowo-dan-pejabat-negara-lainnya.

Identity, VIDA Digital. "Penipuan Deepfake Indonesia Melonjak 1550%: Begini Cara VIDA Memeranginya." *VIDA Digital Identity*, October 2024. https://vida.id/id/pressrelease/penipuan-deepfake-indonesia-melonjak-1550-begini-cara-vida-memeranginya.

Komdigi, Biro Humas Kementerian. "Marak Penipuan Dengan AI, Wamenkomdigi Nezar Patria Minta Masyarakat Waspada." *Komdigi*, April 13, 2025. http://komdigi.go.id/berita/siaran-pers/detail/marak-penipuan-dengan-ai-wamenkomdigi-nezar-patria-minta-masyarakat-waspada.

Kornelius Benuf, Muhamad Azhar. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Staf Badan Konsultasi Hukum, Fakultas Hukum Universitas Diponegoro* 7, no. 1 (2020): 1–14. https://www.scribd.com/document/511815132/Jurnal-MPH-Metodologi-Penelitian-Hukum-Sebagai-Instrumen-Mengurai-Permasalahan-Hukum-Kontemporer?

Polri, Pusiknas Bareskrim. "Tim Siber Ungkap Teknologi Deepfake Catut Nama Pejabat Negara." *Pusiknas Bareskrim Polri*, January 31, 2025. https://pusiknas.polri.go.id/detail_artikel/tim_siber_ungkap_teknologi_deepfake_catut_nama_pejabat_negara.

Polri, Tribratanews. "Penyebar Deepfake Presiden Ditangkap, Sudah Raih Keuntungan Hingga Rp65 Juta." Jakarta, 2025. https://tribratanews.polri.go.id/blog/hukum-4/penyebar-deepfake-presiden-ditangkap-sudah-raih-keuntungan-hingga-rp65-juta-83865.

Tempo. "Polisi Ungkap Modus Penipuan Yang Gunakan Video Presiden Prabowo Subianto." *Tempo*, January 2025. https://www.tempo.co/arsip/polisi-ungkap-modus-penipuan-yang-gunakan-video-presiden-prabowo-subianto-~1197972.

Wibowo, Agus, and Sri Yulianingsih. *Hukum Teknologi Informasi. Yayasan Prima Agus Teknik Bekerja Sama Dengan Universitas Sains & Teknologi Komputer (Universitas STEKOM)*. Semarang: Yayasan Prima Agus Teknik Bekerja sama dengan Universitas Sains & Teknologi Komputer (Universitas STEKOM), 2025.

https://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/578.

Peraturan Perundang-Undangan dan Sumber Hukum Lainnya

Kitab Undang-Undang Hukum Pidana (KUHP)

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

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

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

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi