



Pertanggungjawaban pidana pengembang *artificial intelligence* atas penyalahgunaan teknologi *deepfake* di Indonesia

Tji Natalia Budiman¹, Hernawati RAS²

^{1,2}Universitas Langlangbuana

email: ¹tjinatalia@yahoo.com, ²hernawatiras57@gmail.com

Info Artikel :

Diterima :

13 November 2025

Disetujui :

15 Desember 2025

Dipublikasikan :

25 Januari 2026

ABSTRAK

Maraknya penggunaan teknologi *deepfake* yang menimbulkan risiko serius terhadap reputasi, privasi, dan keamanan masyarakat, sementara regulasi yang mengatur tanggung jawab pengembang masih belum jelas. Tujuan penelitian ini adalah untuk menganalisis kerangka hukum yang dapat diterapkan pada pengembang AI, mengidentifikasi hambatan hukum dalam menegakkan pertanggungjawaban, serta memberikan rekomendasi regulasi yang seimbang antara inovasi teknologi dan perlindungan masyarakat. Metode yang digunakan adalah penelitian yuridis normatif, dengan bahan hukum primer berupa UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, bahan hukum sekunder berupa buku, jurnal, dan artikel ilmiah, serta bahan hukum tersier dari ensiklopedia dan Kamus Besar Bahasa Indonesia. Hasil penelitian menunjukkan bahwa pertanggungjawaban pidana pengembang AI memerlukan pembuktian unsur subjektif dan objektif, namun penegakan hukum menghadapi hambatan berupa *legal gap*, keterbatasan kapasitas aparat penegak hukum, dan perubahan teknologi yang cepat. Regulasi yang adaptif dan berbasis prinsip kehati-hatian dapat menjadi solusi untuk menyeimbangkan inovasi teknologi dengan perlindungan masyarakat sekaligus memberikan kepastian hukum bagi semua pihak.

Kata Kunci: Kecerdasan Buatan, Tanggung Jawab Pidana, Teknologi *Deepfake*, Forensik Digital, Kesenjangan Hukum, Perlindungan Data Pribadi

ABSTRACT

The widespread use of deepfake technology poses serious risks to reputation, privacy, and public security, while regulations governing developer liability remain unclear. The purpose of this study is to analyze the legal framework applicable to AI developers, identify legal barriers to enforcing accountability, and provide regulatory recommendations that balance technological innovation and public protection. The method used is normative legal research, using primary legal materials in the form of Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection; secondary legal materials in the form of books, journals, and scientific articles; and tertiary legal materials from encyclopedias and the Great Indonesian Dictionary. The results show that criminal liability for AI developers requires proof of objective and objective elements. However, law enforcement faces obstacles such as legal gaps, limited capacity of law enforcement officers, and rapid technological change. Adaptive regulations based on the principle of prudence can be a solution to balance technological innovation with public protection while providing legal certainty for all parties. Keywords: Criminal Liability, Artificial Intelligence, Deepfake Technology.

Keywords: Artificial Intelligence, Criminal Liability, Deepfake Technology, Digital Forensics, Legal Gap, Personal Data Protection



©2026 Tji Natalia Budiman, Hernawati RAS. Diterbitkan oleh Arka Institute. Ini adalah artikel akses terbuka di bawah lisensi Creative Commons Attribution NonCommercial 4.0 International License. (<https://creativecommons.org/licenses/by-nc/4.0/>)

PENDAHULUAN

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*, AI) dalam beberapa tahun terakhir telah membawa dampak signifikan terhadap berbagai aspek kehidupan manusia. Salah satu inovasi AI yang menimbulkan kontroversi adalah teknologi *deepfake*, yaitu teknik manipulasi audio-visual yang mampu mereplikasi wajah, suara, dan gerak tubuh seseorang secara realistis tanpa

persetujuan pihak yang bersangkutan.¹ Teknologi ini awalnya dipandang sebagai inovasi positif yang dapat dimanfaatkan dalam industri hiburan, perfilman, pendidikan, dan seni digital. Namun, seiring dengan meluasnya akses terhadap teknologi ini, *deepfake* mulai disalahgunakan untuk berbagai tujuan kriminal, seperti pembuatan konten pornografi non-konsensual, penyebaran hoaks politik, pencemaran nama baik, dan pemerasan digital. Fenomena ini menimbulkan ancaman serius terhadap hak privasi, reputasi individu, serta integritas informasi publik.²

Di Indonesia, kasus-kasus penyalahgunaan *deepfake* telah muncul di berbagai platform daring dan menimbulkan dampak signifikan terhadap individu maupun masyarakat secara luas.³ Teknologi ini memungkinkan pihak-pihak tertentu memanipulasi wajah, suara, dan gerak tubuh seseorang sehingga seolah-olah orang tersebut melakukan atau mengatakan sesuatu yang sebenarnya tidak terjadi. Penyebaran video *deepfake* yang menyesatkan ini menimbulkan risiko serius terhadap reputasi, keamanan, dan kepercayaan publik terhadap informasi yang beredar.

Meskipun Indonesia telah memiliki UU No. 19 Tahun 2016 Tentang Perubahan Atas UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang selanjutnya dalam jurnal ini disebut UU-ITE serta UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, regulasi yang ada belum secara spesifik mengatur tanggung jawab pidana pengembang teknologi AI yang menjadi sumber munculnya *deepfake*. Selama ini, hukum lebih menargetkan pelaku penyebar konten, bukan pencipta algoritma atau sistem AI yang dimanfaatkan secara ilegal.⁴

Ketiadaan regulasi yang jelas ini menimbulkan *legal gap*, yaitu ketidakpastian hukum yang berimplikasi pada kesulitan penegakan hukum. Korban penyalahgunaan *deepfake* sering mengalami kesulitan dalam menuntut keadilan, sementara pelaku memanfaatkan celah hukum yang ada. Dalam perspektif hukum pidana, asas legalitas (*nullum crimen sine lege*) menegaskan bahwa seseorang tidak dapat dipidana kecuali tindakannya telah diatur secara tegas dalam undang-undang. Kekosongan regulasi terkait pengembang AI menjadi tantangan signifikan bagi aparat penegak hukum.

Salah satu kasus yang menonjol terjadi pada Januari 2025, yaitu beredarnya video *deepfake* yang menampilkan Presiden Prabowo Subianto seolah-olah mengumumkan program bantuan finansial dari pemerintah. Dalam video tersebut, Presiden Prabowo tampak mengajak masyarakat untuk mendaftar dan menghubungi nomor kontak tertentu. Banyak korban yang percaya dan mentransfer sejumlah uang yang diklaim sebagai biaya administrasi. Namun, setelah dilakukan pengecekan, terbukti bahwa video tersebut merupakan hasil manipulasi menggunakan teknologi *deepfake* dan bukan pernyataan resmi dari Presiden Prabowo.⁵

Kasus lain terjadi pada Agustus 2025, ketika beredar video *deepfake* yang menampilkan Menteri Keuangan Sri Mulyani Indrawati seolah-olah menyatakan bahwa “guru itu beban negara” dalam sebuah forum di Institut Teknologi Bandung. Video ini dengan cepat menyebar di media sosial dan menimbulkan kontroversi di tengah publik. Kementerian Keuangan kemudian menegaskan bahwa

¹ Elang Rinjani Utara and Anis Widyawati, “Analysis of Criminal Law Enforcement on Non-Consensual Deepfake Pornography in the Dissemination of Manipulative Content in Indonesia,” *Al-Jinayah : Jurnal Hukum Pidana Islam* 11, no. 1 (June 29, 2025): 125–53, <https://doi.org/10.15642/aj.2025.11.1.125-153>.

² Muhammad Ilman Abidin, “Legal Review Of Liability From Deepfake Artificial Intelligence That Contains Pornography,” *MIMBAR : Jurnal Sosial Dan Pembangunan* 39, no. 2 (December 29, 2023): 344–52, <https://doi.org/10.29313/mimbar.v39i2.2965>.

³ Muhammad Faqih Faathurrahman and Enni Soerjati Priowirjanto, “Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia,” *Jurnal Indonesia Sosial Teknologi* 3, no. 11 (2022), <https://doi.org/10.59141/jist.v3i11.528>.

⁴ Tesalonika Liony Polandos, Wenly R J Lolong, and Merry Lenda Kumajas, “Pertanggungjawaban Pidana Pelaku Deepfake Porn Menggunakan Artificial Intelligence (AI),” *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana* 7, no. 2 (2025): 217–24.

⁵ 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 (March 4, 2025): 149–64, <https://doi.org/10.59246/aladalah.v3i2.1263>.

pernyataan tersebut tidak pernah disampaikan oleh Sri Mulyani dan bahwa video yang beredar adalah hasil manipulasi teknologi *deepfake*.⁶

Isu perlindungan korban menjadi sangat penting. Identitas korban sering disalahgunakan, reputasi mereka dirusak, dan mereka mengalami tekanan psikologis yang signifikan. Mekanisme kompensasi dan restitusi yang ada saat ini masih lemah karena regulasi belum menempatkan korban *deepfake* sebagai subjek hukum yang secara khusus dilindungi. Persoalan ini menimbulkan perdebatan mengenai batas tanggung jawab moral dan hukum. Haruskah pengembang AI bertanggung jawab atas kelalaian dalam merancang sistem yang memungkinkan penyalahgunaan? Atau sepenuhnya tanggung jawab berada pada pengguna yang menyalahgunakan sistem tersebut? Ketidakjelasan ini menuntut kajian hukum yang komprehensif untuk memberikan kepastian bagi semua pihak.

Selain aspek regulasi, pertanggungjawaban pidana pengembang AI juga menyentuh ranah filsafat hukum, khususnya terkait *mens rea* atau niat jahat. Sulit dibuktikan apakah pengembang memiliki niat agar teknologi ciptaannya disalahgunakan. Banyak pengembang hanya bermaksud menciptakan inovasi teknologi, sementara hasilnya dimanfaatkan pihak lain untuk tindakan kriminal.⁷

Di ranah internasional, beberapa negara sudah mulai merespons isu pertanggungjawaban pengembang AI. Uni Eropa sedang merancang *EU AI Act*, yang membagi tanggung jawab antara pengembang, penyedia, dan pengguna berdasarkan tingkat risiko teknologi. Regulasi semacam ini menjadi acuan penting bagi Indonesia untuk mengembangkan kerangka hukum yang adaptif terhadap perkembangan teknologi. Indonesia juga telah mengeluarkan Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Penggunaan Kecerdasan Buatan. Surat edaran ini berfungsi sebagai pedoman moral bagi pengembang dan pengguna AI, tetapi tidak memiliki kekuatan hukum yang memaksa. Hal ini menunjukkan perlunya regulasi yang lebih konkret dan berorientasi pada kepastian hukum.

Penegakan hukum juga menghadapi kendala teknis. Bukti digital dapat dimanipulasi atau dihapus dengan mudah, identitas pelaku sulit dilacak, dan kapasitas aparat penegak hukum dalam forensik digital masih terbatas. Hal ini mempersulit proses penuntutan terhadap pengembang AI yang lalai atau yang teknologinya dimanfaatkan secara ilegal.⁸ Kompleksitas bertambah ketika kasus melibatkan yurisdiksi lintas negara. *Deepfake* dapat dibuat di luar negeri dan disebarluaskan melalui server internasional, tetapi dampaknya menimpa warga negara Indonesia. Ketentuan hukum nasional sering kali tidak mampu menjangkau pelaku di luar wilayah hukum Indonesia. Selain itu, muncul konflik antara hak atas privasi individu dan kebebasan berekspresi masyarakat. Regulasi hukum harus mampu menyeimbangkan hak individu untuk melindungi identitas dan kehormatan dengan hak masyarakat untuk berkarya dan mengekspresikan diri di dunia digital.⁹ Urgensi penelitian ini tidak hanya berkaitan dengan hukum pidana semata, tetapi juga melibatkan perlindungan hak asasi manusia, martabat individu, dan menjaga kepercayaan masyarakat terhadap kemajuan teknologi digital.

Beberapa penelitian normatif di Indonesia mulai membahas persoalan ini. Fauzyah (2024)¹⁰ dalam kajiannya menyebutkan bahwa UU No. 19 Tahun 2016 Tentang Perubahan Atas UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang selanjutnya dalam artikel ini disebut UU-ITE dan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi hanya dapat menjerat penyebar konten, namun tidak mengatur pertanggungjawaban pidana pengembang AI secara spesifik. Hal ini

⁶ 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), <https://jicnusantara.com/index.php/jiic/article/view/3787>.

⁷ Ari Ardian Rishadi, M Mulyadi, and Payaman Simanjuntak, "Model Penanganan Kejahatan Teknologi Finansial (Fintech) Dalam Upaya Mendukung Pembangunan Nasional Di Sektor Ekonomi Di Era Digital 4.0," *Jurnal Hukum Positum* 7, no. 1 (2022): 25–42.

⁸ Muhammad Tan Abdul Rahman Haris and Tantimin Tantimin, "Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia," *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (2022): 307–16, <https://doi.org/10.23887/jkh.v8i1.44408>.

⁹ Meirza Aulia Chairani, Krista Yitawati, and Angga Pramodya Pradhana, "Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake," *Jurnal Rechtsens* 13, no. 1 (2024): 81–96, <https://doi.org/10.56013/rechtsens.v13i1.2668>.

¹⁰ Rizgita Nurul Fauzyah, Putri Hafidati, and Sunarya Sunarya, "Perlindungan Hukum Terhadap Korban Tindak Pidana Pembuatan Video Pornografi Palsu (Deepfake Porn) Berbasis Artificial Intelligence Di Indonesia," *Lex Veritatis* 3, no. 3 (2024): 74–88.

menimbulkan dilema dalam menentukan subjek hukum yang tepat ketika teknologi tersebut disalahgunakan.

Penelitian-penelitian sebelumnya mengenai penyalahgunaan teknologi *deepfake* di Indonesia umumnya masih berfokus pada pertanggungjawaban pelaku penyebaran atau pengguna akhir konten, dengan pendekatan deskriptif normatif yang menitikberatkan pada penerapan UU ITE dan UU Perlindungan Data Pribadi. Kajian tersebut belum secara komprehensif menganalisis posisi pengembang *Artificial Intelligence* sebagai subjek hukum yang berpotensi dimintai pertanggungjawaban pidana, serta belum mengembangkan konstruksi teoretis mengenai pembuktian unsur kesalahan (*mens rea*), hubungan kausalitas, dan penerapan asas *geen straf zonder schuld* dalam konteks teknologi berbasis algoritma. Selain itu, sebagian besar penelitian belum mengintegrasikan pendekatan komparatif internasional atau menawarkan model regulasi yang konkret untuk menutupi kekosongan hukum (*legal gap*), sehingga diskursus akademik masih terbatas pada identifikasi masalah tanpa formulasi solusi normatif yang sistematis.

Penelitian ini memiliki kebaruan dengan menempatkan pengembang *Artificial Intelligence* sebagai subjek hukum potensial dalam konstruksi pertanggungjawaban pidana atas penyalahgunaan teknologi *deepfake*, serta menganalisisnya melalui integrasi unsur subjektif dan objektif dalam hukum pidana Indonesia. Berbeda dari penelitian sebelumnya, kajian ini tidak hanya mengidentifikasi kekosongan regulasi, tetapi juga menawarkan pendekatan berbasis prinsip kehati-hatian (*due diligence*) dan analisis risiko sebagai model konseptual untuk menyeimbangkan inovasi teknologi dan perlindungan masyarakat. Penelitian ini diharapkan memberikan rekomendasi regulasi yang dapat menjembatani kesenjangan hukum saat ini.

Berdasarkan permasalahan mengenai kekosongan pengaturan pertanggungjawaban pidana pengembang *Artificial Intelligence* atas penyalahgunaan teknologi *deepfake*, penelitian ini bertujuan untuk: (1) menganalisis konstruksi pertanggungjawaban pidana pengembang AI dalam kerangka hukum positif Indonesia, khususnya berdasarkan UU Informasi dan Transaksi Elektronik dan UU Perlindungan Data Pribadi; (2) mengidentifikasi hambatan yuridis dan teknis dalam penegakan pertanggungjawaban pidana terhadap pengembang AI; serta (3) merumuskan model regulasi yang ideal dan adaptif untuk menyeimbangkan inovasi teknologi dengan perlindungan hak-hak masyarakat. Tujuan tersebut dirumuskan untuk menjawab persoalan krusial mengenai siapa yang dapat dimintai pertanggungjawaban ketika teknologi *deepfake* disalahgunakan dan bagaimana batas tanggung jawab tersebut ditentukan dalam perspektif hukum pidana.

Dengan demikian, penelitian ini diharapkan dapat membantu merumuskan bentuk pertanggungjawaban pidana yang tepat bagi pengembang AI melalui pendekatan hukum positif, komparatif internasional, dan analisis normatif. Kajian ini diharapkan dapat memberikan kontribusi teoretis terhadap pengembangan doktrin pertanggungjawaban pidana dalam konteks teknologi berbasis algoritma, serta kontribusi praktis bagi pembentuk kebijakan dalam menyusun regulasi AI yang lebih responsif dan berorientasi pada perlindungan masyarakat. Kajian ini diharapkan dapat merumuskan bentuk pertanggungjawaban pidana yang tepat bagi pengembang AI, baik melalui pendekatan hukum positif, komparatif internasional, maupun pendekatan normatif.¹¹

Dengan demikian, pemahaman mengenai pertanggungjawaban pidana pengembang AI atas penyalahgunaan teknologi *deepfake* sangat penting untuk memberikan kepastian hukum bagi korban dan menciptakan regulasi yang mampu menyesuaikan dengan dinamika teknologi modern.

METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian hukum yuridis normatif dengan pendekatan peraturan-undangan (pendekatan undang-undang), pendekatan kontekstual (pendekatan konseptual), dan pendekatan komparatif (pendekatan komparatif). Sumber data yang digunakan berupa bahan hukum primer, meliputi UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya dalam UU No. 1 Tahun 2024, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta ketentuan hukum pidana lain yang relevan; bahan hukum sekunder berupa buku, jurnal ilmiah, dan hasil penelitian terkait; serta bahan hukum tersier berupa kamus hukum dan ensiklopedia. Teknik

¹¹ Sabrina Nur Syahirah and Bayu Prasetyo, "Tinjauan Yuridis Terhadap Penggunaan Teknologi Deepfake Untuk Pornografi Melalui Artificial Intelligence (AI) Di Indonesia," *Jurnal Inovasi Hukum Dan Kebijakan* 6, no. 1 (2025).

pengumpulan data dilakukan melalui studi kepustakaan dengan penelusuran dan inventarisasi bahan-bahan hukum yang relevan. Teknik analisis data dilakukan secara kualitatif dengan metode interpretasi sistematis dan argumentatif untuk menganalisis konstruksi pertanggungjawaban pidana pengembang *Artificial Intelligence* dalam konteks teknologi *deepfake*.

HASIL DAN PEMBAHASAN

Analisis Kerangka Hukum Pertanggungjawaban Pidana Pengembang *Artificial Intelligence* dalam Penyalahgunaan Teknologi *Deepfake* di Indonesia

Pertanggungjawaban pidana pengembang *Artificial Intelligence* dalam konteks penyalahgunaan teknologi *deepfake* di Indonesia harus dianalisis melalui kerangka hukum pidana yang berlaku serta prinsip-prinsip dasar pertanggungjawaban, yaitu *geen straf zonder schuld*, yang menekankan bahwa tidak ada pidana tanpa kesalahan.¹² Dengan demikian, unsur subjektif maupun objektif menjadi kunci dalam menentukan apakah pengembang dapat dimintai pertanggungjawaban secara pidana.

Dari aspek objektif, pengembang dapat dimintai pertanggungjawaban pidana apabila terdapat hubungan kausal antara tindakan pengembangan teknologi dan akibat yang ditimbulkan, misalnya kerugian materiil, pencemaran nama baik, atau penyebaran disinformasi.¹³ Pembuktian aspek objektif memerlukan dokumentasi teknis mengenai cara kerja algoritma, riwayat pengembangan, serta bukti penyalahgunaan oleh pihak ketiga. Hal ini menjadi dasar hukum untuk menegakkan pertanggungjawaban pidana secara efektif.¹⁴

UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya menjadi acuan utama untuk menindak penyalahgunaan konten digital di Indonesia. Pasal 27 ayat (1) UU ITE melarang penyebaran informasi elektronik yang merugikan pihak lain, sedangkan Pasal 45 ayat (1) mengatur sanksi pidana bagi pelanggaran tersebut. Meski demikian, UU ini belum secara eksplisit mengatur pertanggungjawaban pengembang AI, sehingga muncul *legal gap* yang menimbulkan kesulitan dalam menjerat pengembang apabila teknologi yang mereka ciptakan digunakan untuk tujuan kriminal.¹⁵

Selain UU ITE, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan kerangka hukum terkait penggunaan data pribadi dalam pembuatan konten *deepfake*. Pengembang yang lalai dalam menerapkan prinsip *privacy by design* atau gagal melakukan mitigasi risiko dapat dimintai pertanggungjawaban jika teknologi mereka digunakan untuk melanggar privasi dan hak individu. Regulasi ini menekankan kewajiban pengembang untuk memastikan keamanan dan integritas data yang menjadi input AI.

Analisis hukum juga menyoroti peran pengembang dalam membangun fitur pencegahan penyalahgunaan. Upaya preventif ini meliputi penerapan sistem verifikasi konten, pembatasan distribusi, audit keamanan algoritma, dan edukasi pengguna. Bukti bahwa pengembang telah mengambil langkah-langkah preventif dapat menjadi faktor mitigasi dalam proses hukum dan menunjukkan kepatuhan terhadap prinsip kehati-hatian (*due diligence*).

Selain aspek hukum nasional, praktik internasional dapat menjadi rujukan. Negara-negara seperti Amerika Serikat, Inggris, dan Uni Eropa telah mulai mengatur tanggung jawab pengembang teknologi melalui pedoman etika AI dan peraturan terkait penyebaran konten digital yang

¹² Yolanda Frisky Amelia, Arfan Kaimuddin, and Hisbul Luthfi Ashsyarofi, "Pertanggungjawaban Pidana Pelaku Terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake Menurut Hukum Positif Indonesia," *Dinamika* 30, no. 1 (2024): 9675–91.

¹³ Fasa Muhammad Hapid, Ija Suntana, and Muhammad Yayan Royani, "Penerapan Asas Geen Straf Zonder Schuld Dalam Penindakan Terhadap Kejahatan Penyalahgunaan Teknologi Deepfake," *Jurnal USM Law Review* 7, no. 3 (2024): 1155–74.

¹⁴ Sarah Amanda Uly Sijabat and Diana Lukitasari, "Konten Gambar Dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik," *Recidive: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan* 13, no. 2 (2024): 179–94, <https://doi.org/10.20961/recidive.v13i2.86771>.

¹⁵ Dewi Asri Puannandini et al., "Liabilitas Produk Ai Dalam Sistem Hukum Indonesia: Implikasi Bagi Pengembang, Pengguna, Dan Penyedia Layanan," *Iuris Studia: Jurnal Kajian Hukum* 6, no. 1 (2025): 24–33.

menyesatkan.¹⁶ Standar internasional ini dapat membantu Indonesia dalam menyusun regulasi yang lebih spesifik dan menutup *legal gap* terkait tanggung jawab pengembang AI.

Peran pengguna teknologi *deepfake* juga relevan. Pengembang tidak dapat sepenuhnya mengontrol semua penyalahgunaan, tetapi mereka memiliki kewajiban untuk membangun fitur keamanan yang meminimalkan potensi penyalahgunaan. Dengan demikian, tanggung jawab pengembang bersifat komplementer terhadap perilaku pengguna.

Perlindungan hukum terhadap korban menjadi bagian integral dari analisis pertanggungjawaban pidana. Korban memiliki hak untuk meminta penghapusan konten, menuntut ganti rugi, dan memperoleh rehabilitasi psikologis. Hal ini menegaskan perlunya mekanisme hukum yang tidak hanya menjerat pengembang, tetapi juga memberikan perlindungan nyata bagi masyarakat.

Kolaborasi antara pemerintah, pengembang, aparat penegak hukum, dan masyarakat diperlukan untuk menciptakan ekosistem digital yang aman dan bertanggung jawab. Pedoman etika, standar teknis, dan regulasi yang jelas menjadi kunci untuk menegakkan pertanggungjawaban pidana secara efektif dan mencegah penyalahgunaan teknologi di masa depan.

Kesimpulannya, pengembang AI dapat dimintai pertanggungjawaban pidana apabila terbukti adanya unsur kesalahan subjektif maupun objektif dalam penyalahgunaan teknologi *deepfake*. Regulasi saat ini belum secara spesifik mengatur tanggung jawab pengembang secara tegas, sehingga pengembangan hukum dan praktik terbaik sangat diperlukan untuk memberikan kepastian hukum dan perlindungan bagi korban.

Hasil penelitian ini menunjukkan bahwa pertanggungjawaban pidana pengembang AI harus dianalisis berdasarkan pemenuhan unsur subjektif dan objektif, serta hubungan kausal antara desain teknologi dan akibat yang ditimbulkan. Temuan ini sejalan dengan penelitian sebelumnya yang menegaskan bahwa prinsip *geen straf zonder schuld* tetap menjadi fondasi utama dalam menentukan tanggung jawab pidana dalam kejahatan siber, termasuk yang melibatkan sistem berbasis algoritma.¹⁷ Selain itu, Penelitian lainnya menyatakan bahwa dalam konteks teknologi digital, pembuktian unsur objektif membutuhkan dukungan audit teknis dan dokumentasi sistem guna menelusuri kontribusi pengembang terhadap timbulnya kerugian.¹⁸ Dengan demikian, penelitian ini memperkuat pandangan bahwa konstruksi hukum pidana konvensional masih dapat diterapkan, namun harus disertai pendekatan pembuktian berbasis teknologi.

Hambatan Hukum Yang Dihadapi Dalam Menegakkan Pertanggungjawaban Pengembang Artificial Intelligence Atas Penyalahgunaan Teknologi Deepfake

Penegakan pertanggungjawaban pidana terhadap pengembang *Artificial Intelligence* atas penyalahgunaan teknologi *deepfake* di Indonesia menghadapi berbagai hambatan substantif dan praktis yang kompleks. Salah satu hambatan utama adalah ketidakjelasan regulasi mengenai tanggung jawab pengembang teknologi. UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, meskipun mengatur larangan penyebaran konten merugikan, tidak secara eksplisit menyorot pengembang sebagai subjek hukum. Akibatnya, aparat penegak hukum sering menemui kesulitan dalam menetapkan batas tanggung jawab antara pengembang, pengguna, dan pihak ketiga yang memanfaatkan teknologi.

Hambatan berikutnya adalah kesulitan pembuktian unsur kesalahan subjektif (*mens rea*). Pengembang tidak selalu mengetahui niat jahat pengguna atau potensi penyalahgunaan teknologi yang mereka ciptakan.¹⁹ Hukum pidana mensyaratkan adanya niat atau kelalaian pengembang agar pertanggungjawaban dapat diterapkan. Membuktikan bahwa pengembang mengetahui potensi

¹⁶ Adnasohn Aqilla Respati, "Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation," *Jurnal USM Law Review* 7, no. 3 (2024): 1737–58.

¹⁷ Muhammad Syafiq Wafi, Aloysius Wisnubroto, and Yudi Prayudi, "Artificial Intelligence-Based Deepfake Crimes: A Conception of Culpability Principle as a Criminal Liability Reform," *Reformasi Hukum* 29, no. 2 (2025): 168–83, <https://doi.org/10.46257/jrh.v29i2.1304>.

¹⁸ Mohammad Rezza Fahlevvi, Kadek Agus Prasdya Indra Kusuma, and Muhammad Wahyu Anugerah, "Integrasi Teknologi Digital Dalam Pengawasan Internal Inspektorat Daerah Kabupaten Gianyar," *JURNAL SYNTAX IMPERATIF: Jurnal Ilmu Sosial Dan Pendidikan* 6, no. 2 (2025): 236–49, <https://doi.org/10.54543/syntaximperatif.v6i2.687>.

¹⁹ Yuli Astiti, "Analisis Yuridis Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Narkotika Berbasis Keadilan Substantif (Studi Putusan No. 667/Pid. Sus/2022/Pn Smg)" (Universitas Islam Sultan Agung Semarang, 2024).

penyalahgunaan dan tetap membiarkan teknologi digunakan secara merugikan menjadi tantangan utama, terutama ketika teknologi AI disebarluaskan secara massal atau dijual tanpa kontrol penuh.

Aspek objektif pun menimbulkan hambatan. Teknologi *deepfake* menggunakan algoritma yang kompleks sehingga dibutuhkan keahlian khusus untuk membuktikan hubungan kausal antara pengembangan teknologi dan kerugian yang muncul. Dalam praktiknya, pihak ketiga yang memodifikasi teknologi dapat menambah kerumitan dalam menetapkan siapa yang dapat dimintai pertanggungjawaban pidana. Tanpa bukti teknis yang memadai, pengembang yang lalai atau sengaja dapat lolos dari penegakan hukum.

Keterbatasan kapasitas aparat penegak hukum juga menjadi kendala signifikan. Aparat penegak hukum membutuhkan pemahaman teknis dan sumber daya memadai untuk memeriksa bukti digital, menganalisis algoritma AI, dan melakukan investigasi forensik terhadap konten *deepfake*.²⁰ Tanpa kemampuan ini, proses hukum menjadi lambat dan efektivitas penegakan pertanggungjawaban pidana terhadap pengembang berkurang.

Perbedaan antara standar internasional dan nasional juga memengaruhi penegakan hukum. Beberapa negara telah menetapkan pedoman etika AI dan regulasi spesifik terkait penyebaran konten digital menyenatkan, sementara Indonesia masih mengandalkan UU ITE dan UU Perlindungan Data Pribadi yang kurang rinci dalam aspek AI. Ketidakharmonisan standar ini menimbulkan kesulitan jika teknologi dikembangkan di luar negeri tetapi disalahgunakan di Indonesia.

Kurangnya pedoman etika dan standar pengembangan AI nasional menjadi faktor penghambat lainnya. Tanpa pedoman yang jelas, pengembang tidak memiliki rujukan hukum dan teknis untuk memitigasi risiko penyalahgunaan. Hal ini menyulitkan pembuktian kelalaian pengembang, karena mereka dapat berargumen bahwa tidak ada kewajiban preventif yang diatur secara spesifik dalam hukum nasional.

Hambatan hukum muncul terkait perlindungan korban. Meskipun UU ITE dan UU Perlindungan Data Pribadi memberikan hak bagi korban, mekanisme penegakan hak-hak tersebut masih terbatas. Korban sering menghadapi kesulitan dalam meminta penghapusan konten, menuntut ganti rugi, atau membuktikan kerugian psikologis dan reputasi akibat penyalahgunaan teknologi.

Perkembangan teknologi AI dan *deepfake* yang sangat cepat menimbulkan hambatan tambahan. Regulasi dan standar hukum sering tertinggal dibanding kemajuan algoritma, sehingga pengembang mungkin tidak sepenuhnya memahami kewajiban hukum saat merancang teknologi.²¹ Ketidakpastian hukum ini mempersulit aparat penegak hukum dalam menetapkan pertanggungjawaban.

Akhirnya, kurangnya literasi digital di masyarakat dan aparat penegak hukum turut memperlambat proses penegakan hukum. Minimnya pemahaman mengenai mekanisme *deepfake*, dampak penyalahgunaan, dan metode pembuktian teknis membuat pengembang atau pihak lain dapat menghindari sanksi.²² Secara keseluruhan, hambatan hukum dalam menegakkan pertanggungjawaban pidana pengembang AI atas penyalahgunaan *deepfake* meliputi regulasi yang belum spesifik, kesulitan pembuktian subjektif dan objektif, keterbatasan kapasitas aparat penegak hukum, perbedaan standar internasional, kurangnya pedoman etika, dan perubahan teknologi yang cepat. Penanganan hambatan ini memerlukan penguatan regulasi, peningkatan kapasitas teknis aparat hukum, pengembangan pedoman etika AI, serta edukasi dan literasi digital bagi masyarakat.

Penelitian ini mengidentifikasi hambatan utama berupa kesulitan pembuktian unsur *mens rea* dan kompleksitas teknis algoritma *deepfake*. Temuan ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa jarak antara pengembang dan pengguna akhir menyulitkan pembuktian unsur kesengajaan atau kelalaian dalam kejahatan berbasis AI.²³ Selain itu, penelitian lain menemukan bahwa

²⁰ Muhamad Nur Ismail, "Pengaruh Teknologi AI Terhadap Evolusi Modus Kejahatan Siber Di Indonesia Tahun 2024–2025 Dan Implikasinya Terhadap Penegakan Hukum," *Jurnal Intelek Dan Cendekiawan Nusantara* 2, no. 6 (2025): 12647–65.

²¹ 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/10.31004/innovative.v5i1.17519>.

²² 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/10.70742/arlash.v2i1.194>.

²³ Sharon Euaggelion Putri Latupeirissa, "Pertanggungjawaban Pidana Dalam Bidang Hak Cipta Hasil Karya AI," 2025.

keterbatasan kapasitas aparat penegak hukum dalam memahami sistem kecerdasan buatan menjadi faktor signifikan dalam terhambatnya proses pembuktian.²⁴ Dengan demikian, hambatan pembuktian dalam penelitian ini konsisten dengan temuan akademik sebelumnya yang menyoroti tantangan teknis dalam penegakan hukum digital.

Model Regulasi Berbasis Risiko dalam Menjamin Pertanggungjawaban Pengembang AI dan Perlindungan Masyarakat

Regulasi memiliki peran strategis dalam menyeimbangkan dorongan inovasi teknologi dengan perlindungan masyarakat dari penyalahgunaan teknologi digital. Dalam konteks *Artificial Intelligence* dan *deepfake*, regulasi tidak hanya berfungsi sebagai alat kontrol, tetapi juga sebagai panduan bagi pengembang agar inovasi tidak melanggar hak-hak masyarakat.²⁵

Pentingnya regulasi terlihat dari potensi risiko yang ditimbulkan oleh teknologi *deepfake*, yang dapat memanipulasi informasi, mencemarkan nama baik, atau memicu kerugian finansial dan psikologis bagi individu. Tanpa regulasi yang jelas, pengembang mungkin tidak memiliki pedoman untuk mencegah penyalahgunaan teknologi yang mereka kembangkan. Di satu sisi, pengembang perlu diberikan ruang untuk berinovasi dan mengembangkan teknologi AI. Di sisi lain, masyarakat harus terlindungi dari risiko yang muncul akibat penyalahgunaan teknologi.²⁶

UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjadi salah satu instrumen hukum utama di Indonesia dalam mengatur konten digital dan informasi elektronik. Meskipun demikian, UU ini belum mengatur secara spesifik pertanggungjawaban pengembang AI. Hal ini menimbulkan kebutuhan untuk regulasi tambahan yang menyesuaikan dengan perkembangan teknologi modern.

Selain UU ITE, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan landasan hukum untuk melindungi informasi pribadi masyarakat yang digunakan dalam teknologi AI. Regulasi ini menekankan kewajiban pengembang untuk menerapkan prinsip *privacy by design* dan melakukan mitigasi risiko penyalahgunaan data.

Regulasi juga dapat mendorong pengembang untuk mengimplementasikan standar etika dalam pengembangan teknologi AI. Standar ini meliputi kewajiban untuk mencegah penyalahgunaan, meminimalkan risiko, dan memastikan transparansi dalam penggunaan algoritma AI. Dengan adanya pedoman etika, pengembang dapat berinovasi secara bertanggung jawab.

Selain itu, regulasi yang jelas membantu aparat penegak hukum dalam menindak kasus penyalahgunaan teknologi *deepfake*. Ketika terdapat aturan yang spesifik mengenai tanggung jawab pengembang, proses pembuktian dan penegakan hukum menjadi lebih terarah dan efektif. Perlindungan masyarakat melalui regulasi tidak hanya terbatas pada aspek hukum pidana, tetapi juga mencakup perlindungan hak asasi manusia, reputasi, dan privasi. Regulasi yang baik harus dapat memastikan masyarakat memiliki mekanisme hukum untuk mengajukan keluhan, meminta penghapusan konten, atau menuntut ganti rugi atas kerugian yang ditimbulkan.

Regulasi dapat mendorong transparansi dan audit terhadap teknologi AI. Pengembang yang diwajibkan untuk melakukan audit algoritma secara berkala dan mendokumentasikan penggunaan teknologi akan lebih bertanggung jawab atas potensi risiko penyalahgunaan. Keseimbangan antara inovasi dan perlindungan masyarakat dapat dicapai melalui kolaborasi multi-stakeholder. Pemerintah, pengembang, akademisi, dan masyarakat perlu bekerja sama untuk merumuskan regulasi yang adaptif terhadap perkembangan teknologi.

Penerapan prinsip *risk-based regulation* menjadi strategi efektif. Regulasi yang berbasis analisis risiko memungkinkan pengembang untuk berinovasi, namun tetap diwajibkan mengantisipasi potensi penyalahgunaan dan kerugian bagi masyarakat. Di sisi lain, regulasi harus fleksibel agar tidak

²⁴ Muhammad Singgih Imam Wibowo and Akhmad Munawar, "Kendala Teknis Dan Hukum Dalam Proses Penyidikan Tindak Pidana Siber Di Indonesia," *Jurnal Hukum Lex Generalis* 5, no. 7 (2024).

²⁵ M Wildan Mufti et al., "Urgensi Pembentukan Peraturan Perundang-Undangan Teknologi Berbasis Artificial Intelligence," *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial* 1, no. 11 (2024), <https://doi.org/10.5281/zenodo.11422903>.

²⁶ Akhmad Zaki Yamani, "Analisis Tantangan Dalam Penyusunan Rancangan Undang-Undang Di Era Transformasi Digital: Antara Regulasi, Inovasi, Dan Perlindungan Hak," *Journal Of Law And Nation* 4, no. 2 (2025): 312–24.

menghambat inovasi. Pembatasan yang terlalu ketat dapat menurunkan daya saing industri teknologi, sedangkan regulasi yang adaptif memungkinkan inovasi berkembang tanpa mengorbankan kepentingan masyarakat. Regulasi juga berfungsi sebagai instrumen edukasi bagi pengembang dan masyarakat. Dengan adanya ketentuan hukum yang jelas, pengembang memahami kewajiban mereka, sementara masyarakat lebih sadar akan hak dan mekanisme perlindungan yang tersedia.

Dalam konteks pertanggungjawaban pidana, regulasi dapat menegaskan kewajiban pengembang untuk melakukan mitigasi risiko dan memastikan penggunaan teknologi tidak merugikan pihak lain. Hal ini penting untuk menutup *legal gap* yang muncul akibat penyalahgunaan teknologi oleh pihak ketiga. Regulasi dapat mendorong pengembangan mekanisme teknologi preventif, seperti sistem deteksi konten palsu, pembatasan distribusi, dan tanda identifikasi konten *deepfake*.²⁷ Langkah-langkah ini tidak hanya melindungi masyarakat, tetapi juga memberikan bukti bahwa pengembang telah menjalankan kewajiban mereka.

Selain itu, regulasi dapat mengatur standar tanggung jawab hukum bagi pengembang. Misalnya, jika teknologi digunakan untuk menyebarkan konten ilegal atau merugikan, pengembang yang lalai dalam menerapkan sistem pengamanan dapat dimintai pertanggungjawaban. Peran regulasi ini penting dalam konteks praktik internasional. Beberapa negara telah menetapkan pedoman etika AI dan regulasi khusus penyebaran konten digital. Indonesia dapat menyesuaikan regulasi nasional dengan praktik internasional untuk memastikan kepatuhan dan perlindungan masyarakat.

Regulasi yang efektif mendorong pengembang untuk berinovasi secara bertanggung jawab, bukan sekadar memprioritaskan keuntungan. Dengan kerangka hukum yang jelas, inovasi dapat diarahkan pada manfaat sosial, ekonomi, dan teknologi. Selain itu, regulasi harus memfasilitasi penegakan hukum cepat dan tepat, agar setiap kasus penyalahgunaan teknologi dapat ditindak secara efisien. Hal ini meningkatkan kepastian hukum bagi masyarakat dan menumbuhkan kepercayaan publik terhadap teknologi. Akhirnya, regulasi berfungsi sebagai mekanisme keseimbangan yang menjaga ekosistem digital sehat. Inovasi teknologi tetap dapat berkembang, sementara masyarakat terlindungi dari risiko yang timbul akibat penyalahgunaan teknologi *deepfake*.

Berdasarkan hasil analisis, diperlukan pembentukan regulasi khusus atau revisi terbatas terhadap UU ITE yang secara eksplisit mengatur pertanggungjawaban pengembang *Artificial Intelligence*, khususnya terkait teknologi *deepfake*. Regulasi tersebut sebaiknya mengadopsi pendekatan *risk-based regulation* dengan klasifikasi tingkat risiko teknologi AI, sehingga kewajiban hukum pengembang disesuaikan dengan potensi dampak yang ditimbulkan. Selain itu, perlu ditegaskan kewajiban hukum berupa penerapan *mandatory algorithmic audit*, dokumentasi pengembangan sistem, penerapan *watermarking* atau penanda digital pada konten sintesis, serta mekanisme *notice and takedown* yang responsif terhadap aduan masyarakat. Pemerintah juga perlu membentuk lembaga pengawas atau otoritas khusus AI yang memiliki kewenangan melakukan evaluasi, sertifikasi, dan penegakan sanksi administratif sebelum masuk ke ranah pidana. Dengan langkah konkret tersebut, regulasi tidak hanya bersifat normatif dan deklaratif, tetapi benar-benar memberikan kepastian hukum, menutup kekosongan norma, serta menciptakan keseimbangan yang proporsional antara inovasi teknologi dan perlindungan hak-hak masyarakat.

Hasil penelitian ini menegaskan bahwa pendekatan regulasi berbasis risiko merupakan model yang relevan untuk menyeimbangkan inovasi dan perlindungan masyarakat. Temuan ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa regulasi berbasis risiko memungkinkan diferensiasi kewajiban hukum sesuai tingkat potensi dampak teknologi.²⁸ Selain itu, penelitian lainnya menunjukkan bahwa model klasifikasi risiko dalam tata kelola AI memberikan kepastian hukum tanpa hambatan inovasi.²⁹ Dengan demikian, penelitian ini memperkuat argumentasi bahwa regulasi berbasis

²⁷ Muh Taufik Darmawan, Amir Junaidi, and Ariy Khaerudin, "Penegakan Hukum Terhadap Penyalahgunaan Deepfake Pada Pornografi Anak Di Era Artificial Intelligence Di Indonesia," *Jurnal Penelitian Serambi Hukum* 18, no. 01 (2025): 42–54, <https://doi.org/10.59582/sh.v18i01.1257>.

²⁸ Yamani, "Analisis Tantangan Dalam Penyusunan Rancangan Undang-Undang Di Era Transformasi Digital: Antara Regulasi, Inovasi, Dan Perlindungan Hak."

²⁹ Bintang Rafli Ananta et al., "Analisis Risiko Pelanggaran Data Pribadi Pada Wacana Pengembangan Sistem Ai Analisis Big-Data Pemerintah Dalam Stranas-Ka," *Risalah Hukum* 21, no. 2 (2025): 78–115, <https://doi.org/10.30872/risalah.v21.i2.1885>.

risiko lebih adaptif terhadap perkembangan teknologi dibandingkan pendekatan yang bersifat represif semata.

KESIMPULAN

Penegakan hukum terhadap pengembang AI di Indonesia masih menghadapi tantangan signifikan baik dari segi substantif maupun praktis. Pertanggungjawaban pidana pengembang AI menuntut adanya pembuktian unsur subjektif dan objektif, termasuk kesengajaan atau kelalaian pengembang dalam mencegah penyalahgunaan teknologi, serta hubungan kausal antara tindakan pengembangan dan dampak yang ditimbulkan, baik berupa kerugian materiil, pencemaran nama baik, maupun pelanggaran privasi. Namun, upaya ini terhambat oleh ketidakjelasan regulasi yang belum secara spesifik mengatur tanggung jawab pengembang, keterbatasan kapasitas aparat penegak hukum dalam memeriksa bukti digital dan menganalisis algoritma AI, kesulitan pembuktian unsur kesalahan subjektif maupun objektif, perubahan teknologi yang sangat cepat, serta rendahnya literasi digital di masyarakat dan aparat penegak hukum. Regulasi menjadi instrumen strategis yang dapat menyeimbangkan dorongan inovasi dengan perlindungan masyarakat. Regulasi yang adaptif dan berbasis risiko memungkinkan pengembang untuk tetap berinovasi, namun diwajibkan untuk menerapkan standar etika, mekanisme pencegahan penyalahgunaan, audit algoritma, dan perlindungan data pribadi, sehingga risiko bagi masyarakat dapat diminimalkan. Dengan demikian, keberadaan regulasi yang jelas, fleksibel, dan berbasis prinsip kehati-hatian (*due diligence*) merupakan kunci untuk menciptakan ekosistem digital yang aman, mendorong inovasi teknologi AI secara bertanggung jawab, melindungi hak-hak individu, dan memberikan kepastian hukum bagi semua pihak, termasuk pengembang, pengguna, dan masyarakat luas, sehingga penyalahgunaan teknologi *deepfake* dapat ditekan dan pertanggungjawaban hukum dapat ditegakkan secara efektif.

DAFTAR PUSTAKA

- Abidin, Muhammad Ilman. "Legal Review Of Liability From Deepfake Artificial Intelligence That Contains Pornography." *MIMBAR : Jurnal Sosial Dan Pembangunan* 39, no. 2 (December 29, 2023): 344–52. <https://doi.org/10.29313/mimbar.v39i2.2965>.
- Amelia, Yolanda Frisky, Arfan Kaimuddin, and Hisbul Luthfi Ashsyarofi. "Pertanggungjawaban Pidana Pelaku Terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake Menurut Hukum Positif Indonesia." *Dinamika* 30, no. 1 (2024): 9675–91.
- Ananta, Bintang Rafli, Chanidia Ari Rahmayani, Laga Sugiarto, Anastasya Adityawati Nugroho, and Shabrina Assalamah. "Analisis Risiko Pelanggaran Data Pribadi Pada Wacana Pengembangan Sistem Ai Analisis Big-Data Pemerintah Dalam Stranas-Ka." *Risalah Hukum* 21, no. 2 (2025): 78–115. <https://doi.org/10.30872/risalah.v21.i2.1885>.
- Astiti, Yuli. "Analisis Yuridis Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Narkotika Berbasis Keadilan Substantif (Studi Putusan No. 667/Pid. Sus/2022/Pn Smg)." Universitas Islam Sultan Agung Semarang, 2024.
- Chairani, Meirza Aulia, Krista Yitawati, and Angga Pramodya Pradhana. "Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake." *Jurnal Rechtsens* 13, no. 1 (2024): 81–96. <https://doi.org/10.56013/rechtsens.v13i1.2668>.
- Darmawan, Muh Taufik, Amir Junaidi, and Ariy Khaerudin. "Penegakan Hukum Terhadap Penyalahgunaan Deepfake Pada Pornografi Anak Di Era Artificial Intelligence Di Indonesia." *Jurnal Penelitian Serambi Hukum* 18, no. 01 (2025): 42–54. <https://doi.org/10.59582/sh.v18i01.1257>.
- Faathurrahman, Muhammad Faqih, and Enni Soerjati Priowirjanto. "Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia." *Jurnal Indonesia Sosial Teknologi* 3, no. 11 (2022). <https://doi.org/10.59141/jist.v3i11.528>.
- Fahlevvi, Mohammad Rezza, Kadek Agus Prasdya Indra Kusuma, and Muhammad Wahyu Anugerah. "Integrasi Teknologi Digital Dalam Pengawasan Internal Inspektorat Daerah Kabupaten

- Gianyar.” *JURNAL SYNTAX IMPERATIF: Jurnal Ilmu Sosial Dan Pendidikan* 6, no. 2 (2025): 236–49. <https://doi.org/10.54543/syntaximperatif.v6i2.687>.
- Fauzyah, Rizgita Nurul, Putri Hafidati, and Sunarya Sunarya. “Perlindungan Hukum Terhadap Korban Tindak Pidana Pembuatan Video Pornografi Palsu (Deepfake Porn) Berbasis Artificial Intelligence Di Indonesia.” *Lex Veritatis* 3, no. 3 (2024): 74–88.
- 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). <https://jicnusantara.com/index.php/jiic/article/view/3787>.
- Hapid, Fasa Muhamad, Ija Suntana, and Muhammad Yayan Royani. “Penerapan Asas Geen Straf Zonder Schuld Dalam Penindakan Terhadap Kejahatan Penyalahgunaan Teknologi Deepfake.” *Jurnal USM Law Review* 7, no. 3 (2024): 1155–74.
- Haris, Muhammad Tan Abdul Rahman, and Tantimin Tantimin. “Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia.” *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (2022): 307–16. <https://doi.org/10.23887/jkh.v8i1.44408>.
- Ismail, Muhamad Nur. “Pengaruh Teknologi AI Terhadap Evolusi Modus Kejahatan Siber Di Indonesia Tahun 2024–2025 Dan Implikasinya Terhadap Penegakan Hukum.” *Jurnal Intelek Dan Cendekiawan Nusantara* 2, no. 6 (2025): 12647–65.
- 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 (March 4, 2025): 149–64. <https://doi.org/10.59246/aladalah.v3i2.1263>.
- Latupeirissa, Sharon Euaggelion Putri. “Pertanggungjawaban Pidana Dalam Bidang Hak Cipta Hasil Karya AI,” 2025.
- Mufti, M Wildan, M Hiroshi Ikhsan, Rafif Sani, and M Fauzan. “Urgensi Pembentukan Peraturan Perundang-Undangan Teknologi Berbasis Artificial Intelligence.” *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial* 1, no. 11 (2024). <https://doi.org/10.5281/zenodo.11422903>.
- Polandos, Tesalonika Liony, Wenly R J Lolong, and Merry Lenda Kumajas. “Pertanggungjawaban Pidana Pelaku Deepfake Porn Menggunakan Artificial Intelligence (AI).” *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana* 7, no. 2 (2025): 217–24.
- 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/10.70742/arlash.v2i1.194>.
- Puannandini, Dewi Asri, Raihan Fabian, Reival Andhika Putra Firdaus, M Zaenal Mustopa, and Indra Herdiyana. “Liabilitas Produk Ai Dalam Sistem Hukum Indonesia: Implikasi Bagi Pengembang, Pengguna, Dan Penyedia Layanan.” *Iuris Studia: Jurnal Kajian Hukum* 6, no. 1 (2025): 24–33.
- Respati, Adnasohn Aqilla. “Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation.” *Jurnal USM Law Review* 7, no. 3 (2024): 1737–58.
- Rishadi, Ari Ardian, M Mulyadi, and Payaman Simanjuntak. “Model Penanganan Kejahatan Teknologi Finansial (Fintech) Dalm Upaya Mendukung Pembangunan Nasional Di Sektor Ekonomi Di Era Digital 4.0.” *Jurnal Hukum Positum* 7, no. 1 (2022): 25–42.
- Sijabat, Sarah Amanda Uly, and Diana Lukitasari. “Konten Gambar Dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik.” *Recidive: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan* 13, no. 2 (2024): 179–94. <https://doi.org/10.20961/recidive.v13i2.86771>.
- Syahirah, Sabrina Nur, and Bayu Prasetyo. “Tinjauan Yuridis Terhadap Penggunaan Teknologi

- Deepfake Untuk Pornografi Melalui Artificial Intelligence (AI) Di Indonesia.” *Jurnal Inovasi Hukum Dan Kebijakan* 6, no. 1 (2025).
- Utara, Elang Rinjani, and Anis Widyawati. “Analysis of Criminal Law Enforcement on Non-Consensual Deepfake Pornography in the Dissemination of Manipulative Content in Indonesia.” *Al-Jinayah: Jurnal Hukum Pidana Islam* 11, no. 1 (June 29, 2025): 125–53. <https://doi.org/10.15642/aj.2025.11.1.125-153>.
- Wafi, Muhammad Syafiq, Aloysius Wisnubroto, and Yudi Prayudi. “Artificial Intelligence-Based Deepfake Crimes: A Conception of Culpability Principle as a Criminal Liability Reform.” *Reformasi Hukum* 29, no. 2 (2025): 168–83. <https://doi.org/10.46257/jrh.v29i2.1304>.
- 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/10.31004/innovative.v5i1.17519>.
- Wibowo, Muhammad Singgih Imam, and Akhmad Munawar. “Kendala Teknis Dan Hukum Dalam Proses Penyidikan Tindak Pidana Siber Di Indonesia.” *Jurnal Hukum Lex Generalis* 5, no. 7 (2024).
- Yamani, Akhmad Zaki. “Analisis Tantangan Dalam Penyusunan Rancangan Undang-Undang Di Era Transformasi Digital: Antara Regulasi, Inovasi, Dan Perlindungan Hak.” *Journal Of Law And Nation* 4, no. 2 (2025): 312–24.