

PERTANGGUNGJAWABAN PIDANA TERHADAP PENYALAHGUNAAN DEEPFAKE ARTIFICIAL INTELLIGENCE DALAM PERSPEKTIF KUHP NASIONAL DAN UNDANG -UNDANG ITE

Ahmad Burhanuddin

UIN Raden Intan Lampung, Indonesia
ahmadburhanuddin@radenintan.ac.id

Karimuddin Hasibuan

Institut Syekh Abdul Halim Hasan Binjai, Indonesia
karimuddinhsb@gmail.com

Chairil Setiadi

UIN Sjech M. Djamil Djambek Bukittinggi, Indonesia
chairilsetiadi@gmail.com

Faldo Aldiano

Universitas Andalas Padang, Indonesia
Aldiano56@gmail.com

Article History:

Received: September 10, 2026;
Accepted: September 30, 2026;
Published: October 07, 2026;

Abstract. *The advancement of Artificial Intelligence (AI) has given rise to deepfake technology capable of manipulating faces, voices, and videos with such realism that they are difficult to distinguish from authentic content. In Indonesia, the misuse of deepfakes has garnered increasing attention following various viral incidents involving the manipulation of public figures' videos, fraud utilizing voice cloning, the dissemination of non-consensual pornography, and the spread of disinformation via digital media—all of which have caused both material and non-material harm. This phenomenon raises questions regarding the adequacy of existing criminal law provisions to prosecute perpetrators and provide legal protection for victims. This study aims to analyze the forms of criminal liability associated with deepfake misuse from the perspectives of the National Criminal Code and the Electronic Information and Transactions (ITE) Law, as well as their relationship with other supporting regulations. The research employs a normative-juridical method utilizing statutory, conceptual, and case-study approaches focused on viral deepfake incidents in Indonesia. Primary, secondary, and tertiary legal materials were analyzed qualitatively through systematic and comparative interpretation techniques. The findings indicate that deepfake misuse potentially satisfies the elements of various criminal offenses—such as the unlawful dissemination of electronic information, fraud, defamation, extortion, and violations of privacy rights—yet existing regulations remain fragmented and do not explicitly address the specific characteristics of AI-based crimes. Consequently, there is a need for adaptive criminal law reform, the harmonization of digital regulations, and the strengthening of electronic evidentiary mechanisms to ensure legal*

certainty, victim protection, and effective law enforcement against deepfake-related crimes in Indonesia.

Keywords:

*Artificial Intelligence;
Cybercrime; Deepfake;
Electronic Evidence;
ITE Law; Indonesian Criminal
Law; National Criminal Code.*

Abstrak. Perkembangan *Artificial Intelligence* (AI) telah melahirkan teknologi *deepfake* yang mampu memanipulasi wajah, suara, dan video secara sangat realistis sehingga sulit dibedakan dari konten autentik. Di Indonesia, penyalahgunaan *deepfake* semakin mendapat perhatian setelah muncul berbagai kasus viral berupa manipulasi video tokoh publik, penipuan menggunakan tiruan suara, penyebaran konten pornografi non-konsensual, serta disinformasi melalui media digital yang menimbulkan kerugian materiil maupun immateriil. Fenomena tersebut memunculkan persoalan mengenai kecukupan pengaturan hukum pidana dalam menjerat pelaku dan memberikan perlindungan hukum kepada korban. Penelitian ini bertujuan menganalisis bentuk pertanggungjawaban pidana terhadap penyalahgunaan *deepfake* dalam perspektif Kitab Undang-Undang Hukum Pidana Nasional dan Undang-Undang Informasi dan Transaksi Elektronik beserta keterkaitannya dengan regulasi pendukung lainnya. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan studi kasus terhadap beberapa fenomena *deepfake* yang viral di Indonesia. Bahan hukum primer, sekunder, dan tersier dianalisis secara kualitatif melalui teknik interpretasi sistematis dan komparatif. Hasil penelitian menunjukkan bahwa penyalahgunaan *deepfake* berpotensi memenuhi unsur berbagai tindak pidana, seperti penyebaran informasi elektronik yang melawan hukum, penipuan, pencemaran nama baik, pemerasan, serta pelanggaran terhadap hak privasi, namun pengaturan yang ada masih bersifat tersebar dan belum secara eksplisit mengakomodasi karakteristik kejahatan berbasis AI. Oleh karena itu, diperlukan pembaruan kebijakan hukum pidana yang adaptif, harmonisasi regulasi digital, serta penguatan mekanisme pembuktian elektronik untuk mewujudkan kepastian hukum, perlindungan korban, dan efektivitas penegakan hukum terhadap kejahatan *deepfake* di Indonesia.

A. PENDAHULUAN

Transformasi digital yang ditandai dengan pesatnya perkembangan *Artificial Intelligence* (AI) telah membawa perubahan mendasar dalam berbagai aspek kehidupan, termasuk komunikasi, ekonomi, pendidikan, pemerintahan, dan penegakan hukum. Salah satu inovasi AI yang berkembang sangat cepat adalah teknologi *deepfake*, yaitu teknik manipulasi audio, gambar, dan video menggunakan algoritma *deep learning* sehingga mampu menghasilkan konten sintetis yang menyerupai kondisi nyata (Cantika et al., 2025). Pada awalnya teknologi ini dikembangkan untuk kebutuhan industri kreatif, perfilman, pendidikan, dan hiburan. Namun, dalam perkembangannya, *deepfake* semakin sering disalahgunakan sebagai sarana melakukan berbagai

bentuk kejahatan digital yang menimbulkan kerugian ekonomi, psikologis, sosial, maupun hukum (Gustawinata et al., 2021).

Penyalahgunaan *deepfake* mulai menjadi perhatian serius seiring meningkatnya kasus manipulasi wajah dan suara tokoh publik, penipuan berbasis *voice cloning*, penyebaran konten pornografi non-konsensual, serta produksi informasi palsu yang beredar secara masif melalui media sosial. Pemerintah melalui Kementerian Komunikasi dan Digital (Komdigi) menegaskan bahwa teknologi AI telah meningkatkan kompleksitas ancaman penipuan digital karena mampu menghasilkan video dan suara palsu yang sulit dibedakan dari konten autentik. Bahkan, data yang disampaikan Komdigi mengutip Sensity AI menunjukkan peningkatan konten *deepfake* secara global hingga sekitar 550% dalam lima tahun terakhir, sementara berbagai modus penipuan berbasis AI juga terus meningkat di Indonesia (Ibrahim et al., 2015).

Fenomena tersebut tidak lagi bersifat hipotetis. Berbagai kasus viral di Indonesia menunjukkan bahwa teknologi AI telah dimanfaatkan untuk membuat konten vulgar berbasis foto pribadi tanpa persetujuan korban, melakukan manipulasi identitas digital, hingga menjalankan modus penipuan yang meniru suara atau wajah seseorang. Salah satu kasus yang memperoleh perhatian publik adalah dugaan pembuatan konten *deepfake* vulgar terhadap mahasiswi di Pontianak yang memunculkan kembali perdebatan mengenai perlindungan hukum korban dan efektivitas instrumen hukum pidana dalam menghadapi kejahatan berbasis AI (Bessoran, 2026). Peristiwa-peristiwa tersebut menunjukkan bahwa perkembangan teknologi digital berlangsung jauh lebih cepat dibandingkan perkembangan regulasi yang mengaturnya.

Penyalahgunaan *deepfake* menimbulkan persoalan yang kompleks karena karakteristik tindakannya tidak selalu dapat diklasifikasikan ke dalam satu jenis tindak pidana. Dalam praktiknya, pelaku dapat dikenakan ketentuan mengenai penipuan, pencemaran nama baik, penyebaran informasi elektronik yang melawan hukum, pemerasan, pornografi, maupun pelanggaran terhadap hak privasi. Akan tetapi, hingga saat ini belum terdapat ketentuan yang secara eksplisit mengatur tindak pidana *deepfake* sebagai bentuk

kejahatan berbasis kecerdasan buatan (M. Fadillah, 2023). Kondisi tersebut berpotensi menimbulkan kekosongan norma (*legal gap*) yang berdampak pada ketidakpastian hukum, khususnya ketika aparat penegak hukum harus menentukan konstruksi pertanggungjawaban pidana terhadap pelaku.

Berlakunya Kitab Undang-Undang Hukum Pidana Nasional memberikan momentum penting dalam pembaruan hukum pidana Indonesia melalui pendekatan yang lebih adaptif terhadap perkembangan masyarakat dan teknologi. Meskipun demikian, pengaturan mengenai penyalahgunaan AI masih tersebar dalam berbagai peraturan, terutama KUHP Nasional, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi, serta regulasi lain yang mengatur transaksi elektronik dan perlindungan hak digital (Pramudiasari, 2024). Fragmentasi pengaturan tersebut menimbulkan tantangan dalam menentukan dasar pertanggungjawaban pidana ketika suatu konten *deepfake* menimbulkan kerugian lintas dimensi, seperti kerugian reputasi, kerugian ekonomi, maupun pelanggaran terhadap hak privasi korban.

Penelitian-penelitian terdahulu pada umumnya masih berfokus pada aspek kriminalisasi *deepfake*, perlindungan data pribadi, atau tanggung jawab platform digital. Kajian yang secara khusus mengintegrasikan perspektif KUHP Nasional dan UU ITE untuk menganalisis konstruksi pertanggungjawaban pidana terhadap penyalahgunaan *deepfake* di Indonesia masih relatif terbatas (Dwi Ika Ardiyani, 2024). Padahal, perkembangan modus kejahatan berbasis AI menuntut formulasi pertanggungjawaban pidana yang mampu mengakomodasi karakteristik baru kejahatan siber sekaligus memberikan kepastian hukum bagi aparat penegak hukum, pelaku, maupun korban.

Berdasarkan kondisi tersebut, penelitian ini menjadi penting untuk menganalisis bentuk pertanggungjawaban pidana terhadap penyalahgunaan *deepfake Artificial Intelligence* dalam perspektif KUHP Nasional dan UU ITE, sekaligus mengidentifikasi kecukupan norma hukum yang berlaku dalam menjawab tantangan kejahatan digital berbasis AI. Hasil penelitian

diharapkan dapat memberikan kontribusi teoritis bagi pengembangan hukum pidana siber di Indonesia serta menjadi rekomendasi kebijakan bagi pembentuk undang-undang dalam merumuskan regulasi yang lebih adaptif terhadap perkembangan teknologi kecerdasan buatan dan perlindungan masyarakat di era digital.

B. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum yuridis normatif dengan pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan digunakan untuk mengkaji ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) Nasional, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta peraturan perundang-undangan lain yang berkaitan dengan tindak pidana siber dan penyalahgunaan teknologi kecerdasan buatan (*Artificial Intelligence*). Pendekatan konseptual digunakan untuk menganalisis teori pertanggungjawaban pidana, asas legalitas, kesalahan (*mens rea*), perlindungan hukum, serta konsep kejahatan siber berbasis AI.

Bahan hukum penelitian terdiri atas bahan hukum primer berupa peraturan perundang-undangan dan putusan pengadilan yang relevan apabila tersedia, bahan hukum sekunder berupa artikel ilmiah, buku, hasil penelitian, serta publikasi lembaga pemerintah, dan bahan hukum tersier berupa kamus hukum, ensiklopedia, dan dokumen pendukung lainnya. Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*) dan penelusuran dokumen digital yang kredibel. Analisis data menggunakan metode analisis kualitatif dengan teknik interpretasi gramatikal, sistematis, dan teleologis untuk mengidentifikasi kecukupan norma hukum dalam mengatur pertanggungjawaban pidana atas penyalahgunaan *deepfake*. Hasil analisis kemudian disajikan secara deskriptif-analitis untuk merumuskan konstruksi

hukum yang adaptif terhadap perkembangan kejahatan berbasis kecerdasan buatan di Indonesia.

C. HASIL DAN PEMBAHASAN

1. Konstruksi Pertanggungjawaban Pidana terhadap Penyalahgunaan *Deepfake Artificial Intelligence* dalam Perspektif KUHP Nasional

Perkembangan *Artificial Intelligence* (AI) telah melahirkan bentuk kejahatan baru melalui teknologi *deepfake* yang mampu merekayasa wajah, suara, maupun video dengan tingkat kemiripan yang sangat tinggi. Berdasarkan analisis terhadap berbagai kasus yang menjadi perhatian publik di Indonesia selama periode 2024–2026, penyalahgunaan *deepfake* tidak lagi dimanfaatkan untuk kepentingan hiburan semata, tetapi telah berkembang menjadi instrumen tindak pidana berupa penipuan, pencemaran nama baik, eksploitasi seksual, manipulasi identitas digital, dan penyebaran informasi palsu (Pasundan, 2026). Karakteristik *deepfake* telah mengubah pola kejahatan siber dari kejahatan berbasis sistem menjadi kejahatan berbasis manipulasi persepsi publik. Perubahan tersebut mengakibatkan meningkatnya kompleksitas pembuktian pidana karena bukti visual dan audio tidak lagi dapat diasumsikan sebagai representasi fakta yang autentik (Rahmawati & Irdianty, 2024). Oleh karena itu, perkembangan AI telah menciptakan tantangan baru bagi sistem hukum pidana Indonesia dalam memberikan perlindungan hukum terhadap masyarakat.

Analisis terhadap data penelitian menunjukkan bahwa sebagian besar penyalahgunaan *deepfake* dilakukan melalui pemanfaatan foto, video, dan rekaman suara yang diperoleh dari media sosial maupun sumber digital lainnya tanpa persetujuan pemiliknya. Konten tersebut kemudian diproses menggunakan algoritma AI generatif sehingga menghasilkan video atau suara sintesis yang menyerupai korban (Wicaksono et al., 2026). Modus operandi pelaku umumnya bertujuan memperoleh keuntungan ekonomi, melakukan pemerasan, merusak reputasi individu tertentu, maupun

menciptakan disinformasi yang memengaruhi opini publik. Korban tidak hanya mengalami kerugian finansial, tetapi juga kehilangan reputasi, mengalami tekanan psikologis, serta menghadapi stigma sosial akibat penyebaran konten yang telah dimanipulasi. Kondisi tersebut menunjukkan bahwa dampak kejahatan *deepfake* bersifat multidimensional sehingga memerlukan pendekatan hukum pidana yang komprehensif (Akbar et al., 2026).

Berdasarkan telaah normatif terhadap KUHP Nasional, penelitian menemukan bahwa meskipun belum terdapat ketentuan yang secara eksplisit mengatur tindak pidana *deepfake*, substansi perbuatan pelaku tetap dapat dikualifikasikan sebagai tindak pidana apabila memenuhi unsur-unsur delik yang telah dirumuskan dalam KUHP. Dalam perspektif hukum pidana, teknologi AI diposisikan sebagai sarana (*instrumentum sceleris*), sedangkan fokus pertanggungjawaban tetap diarahkan kepada manusia sebagai subjek hukum yang menggunakan teknologi tersebut untuk melakukan perbuatan melawan hukum (Gustawinata et al., 2021). Dengan demikian, keberadaan AI tidak menghapus sifat melawan hukum maupun kesalahan pelaku. Pendekatan ini menunjukkan bahwa perkembangan teknologi tidak mengubah prinsip dasar hukum pidana, melainkan memperluas bentuk perbuatan yang dapat dilakukan dengan menggunakan teknologi digital (Haefani & Mulyanti, 2025).

Konstruksi pertanggungjawaban pidana terhadap penyalahgunaan *deepfake* harus didasarkan pada terpenuhinya unsur *actus reus* dan *mens rea*. Unsur *actus reus* diwujudkan melalui tindakan menciptakan, memodifikasi, menyebarluaskan, atau menggunakan konten *deepfake* yang menimbulkan akibat hukum bagi korban maupun masyarakat. Adapun unsur *mens rea* dibuktikan melalui adanya kesengajaan, pengetahuan, atau kehendak pelaku untuk menggunakan teknologi tersebut dalam melakukan tindak pidana (Kurniawan, 2026). Mayoritas kasus *deepfake* di Indonesia dilakukan secara sadar dengan tujuan memperoleh keuntungan ekonomi atau menyerang kehormatan pihak lain. Oleh karena itu, unsur kesalahan

sebagai dasar pertanggungjawaban pidana tetap dapat dibuktikan meskipun tindak pidana dilakukan melalui teknologi berbasis AI.

Penerapan asas legalitas menjadi dasar penting dalam menentukan dapat atau tidaknya pelaku dimintai pertanggungjawaban pidana. Meskipun KUHP Nasional belum mengenal istilah *deepfake*, penelitian menemukan bahwa perbuatan yang dilakukan melalui teknologi tersebut tetap dapat dipidana sepanjang memenuhi rumusan tindak pidana yang telah diatur dalam undang-undang (Beryl Helga Fredella Hibatulloh, 2025). Dengan demikian, penerapan hukum tidak berorientasi pada nama teknologi yang digunakan, melainkan pada sifat melawan hukum dari perbuatan yang dilakukan. Pendekatan tersebut sejalan dengan doktrin hukum pidana modern yang menempatkan perkembangan teknologi sebagai media pelaksanaan tindak pidana, bukan sebagai dasar pembentukan unsur delik baru. Oleh sebab itu, asas legalitas tetap terjaga tanpa menghambat penegakan hukum terhadap kejahatan digital.

Kejahatan *deepfake* memerlukan pendekatan pembuktian yang berbeda dibandingkan tindak pidana konvensional. Penelitian menemukan bahwa bukti berupa video, gambar, dan rekaman suara tidak lagi cukup dinilai berdasarkan pengamatan visual semata, tetapi harus diverifikasi melalui pemeriksaan forensik digital (Hukum, 2026). Pemeriksaan tersebut meliputi analisis metadata, struktur piksel, pola sintesis suara, serta jejak algoritma AI yang digunakan dalam proses manipulasi. Kemampuan aparat penegak hukum dalam melakukan analisis forensik digital menjadi faktor yang sangat menentukan keberhasilan pembuktian di persidangan. Dengan demikian, penguatan kapasitas laboratorium forensik digital merupakan kebutuhan mendesak dalam menghadapi perkembangan kejahatan berbasis AI.

Hubungan kausal antara tindakan pelaku dan akibat yang dialami korban merupakan unsur penting dalam menentukan pertanggungjawaban pidana. Dalam berbagai kasus yang dianalisis, penyebaran konten *deepfake* terbukti menyebabkan kerugian ekonomi, hilangnya kesempatan kerja,

rusaknya reputasi profesional, gangguan psikologis, serta menurunnya kepercayaan publik terhadap korban (Polandos, T.L., Lolong, W.R.J., Kumajas, 2025). Algoritma media sosial mempercepat penyebaran konten sehingga dampak yang ditimbulkan jauh lebih luas dibandingkan tindak pidana konvensional. Oleh karena itu, pembuktian hubungan sebab-akibat antara tindakan manipulasi digital dengan kerugian yang muncul menjadi dasar utama dalam menjatuhkan sanksi pidana terhadap pelaku.

Beberapa kendala dalam penegakan hukum terhadap penyalahgunaan *deepfake* di Indonesia. Kendala tersebut meliputi belum adanya pedoman teknis mengenai identifikasi *deepfake*, keterbatasan sumber daya manusia yang memiliki kompetensi forensik digital, serta minimnya koordinasi antarlembaga dalam penanganan kejahatan siber (Kurniarullah, 2021). Selain itu, sifat lintas negara (*cross-border crime*) dari penyebaran konten digital menyebabkan proses penelusuran pelaku menjadi lebih kompleks. Penelitian juga menemukan bahwa sebagian besar masyarakat belum memiliki literasi digital yang memadai untuk membedakan konten asli dan konten sintesis, sehingga penyebaran *deepfake* berlangsung sangat cepat. Kondisi tersebut menunjukkan perlunya penguatan kapasitas kelembagaan dan peningkatan literasi digital sebagai bagian dari strategi penanggulangan kejahatan berbasis AI.

KUHP Nasional pada prinsipnya masih memiliki kapasitas untuk menjadi dasar pertanggungjawaban pidana terhadap penyalahgunaan *deepfake* melalui penerapan unsur-unsur delik yang telah ada. Namun demikian, penelitian ini menemukan adanya kekosongan norma terkait karakteristik khusus kejahatan berbasis AI yang berpotensi menimbulkan perbedaan interpretasi dalam praktik penegakan hukum (Pasundan, 2026). Oleh karena itu, diperlukan pembaruan kebijakan hukum pidana yang mengakomodasi perkembangan teknologi kecerdasan buatan tanpa mengabaikan asas legalitas dan kepastian hukum. Reformulasi tersebut perlu diarahkan pada penguatan norma mengenai manipulasi identitas digital, pembuktian elektronik berbasis AI, serta perlindungan korban

kejahatan digital. Dengan demikian, sistem hukum pidana Indonesia akan lebih adaptif dalam menghadapi dinamika perkembangan teknologi sekaligus mampu memberikan kepastian hukum dan perlindungan yang efektif bagi masyarakat.

2. Analisis Pertanggungjawaban Pidana Penyalahgunaan *Deepfake Artificial Intelligence* dalam Perspektif UU ITE dan Harmonisasi Hukum Digital Indonesia

Penyalahgunaan *deepfake Artificial Intelligence* merupakan bentuk kejahatan digital yang secara substansial lebih tepat dianalisis menggunakan pendekatan *lex specialis derogat legi generali*, yaitu menempatkan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai instrumen hukum khusus dalam penanganan tindak pidana berbasis sistem elektronik (Dwi Ika Ardiyani, 2024). Berdasarkan analisis terhadap berbagai fenomena *deepfake* yang viral di Indonesia, ditemukan bahwa modus operandi pelaku selalu melibatkan media elektronik sebagai sarana utama dalam pembuatan, penyimpanan, transmisi, maupun distribusi konten sintetis (Pramudiasari, 2024). Oleh karena itu, meskipun KUHP Nasional tetap menjadi dasar umum pertanggungjawaban pidana, UU ITE memiliki fungsi strategis dalam mengatur aspek penggunaan informasi elektronik dan dokumen elektronik sebagai objek maupun alat tindak pidana (Dhyah Nur Fitriana & Ghoniyah Zulindah Maulidya, 2023). Penelitian menemukan bahwa beberapa unsur dalam UU ITE dapat diterapkan terhadap penyalahgunaan *deepfake*, khususnya ketika konten yang dihasilkan mengandung muatan pencemaran nama baik, pemerasan, penipuan elektronik, manipulasi informasi, atau penyebaran informasi yang menimbulkan kerugian bagi orang lain. Temuan ini menunjukkan bahwa penerapan UU ITE tidak hanya berfungsi sebagai

pelengkap KUHP Nasional, tetapi juga sebagai instrumen hukum yang memberikan kepastian dalam menghadapi perkembangan kejahatan digital berbasis kecerdasan buatan. Dengan demikian, konstruksi pertanggungjawaban pidana terhadap pelaku *deepfake* harus dipahami sebagai integrasi antara norma hukum pidana umum dan hukum pidana khusus yang mengatur ruang siber (Weni Aulia & Rayyan, 2024).

Analisis terhadap praktik penegakan hukum menunjukkan bahwa hubungan antara KUHP Nasional dan UU ITE bersifat saling melengkapi dalam menentukan pertanggungjawaban pidana terhadap penyalahgunaan *deepfake*. Hasil penelitian menemukan bahwa KUHP Nasional memberikan landasan mengenai asas legalitas, kesalahan (*schuld*), kemampuan bertanggung jawab, serta tujuan pemidanaan, sedangkan UU ITE mengatur karakteristik tindak pidana yang dilakukan melalui sistem elektronik. Integrasi kedua regulasi tersebut menjadi penting mengingat penyalahgunaan *deepfake* umumnya menimbulkan lebih dari satu akibat hukum, seperti penipuan, pencemaran nama baik, manipulasi identitas digital, penyebaran konten asusila, maupun kerugian ekonomi. Berdasarkan analisis terhadap beberapa perkara yang memperoleh perhatian publik, aparat penegak hukum cenderung menggunakan kombinasi ketentuan KUHP dan UU ITE agar seluruh unsur perbuatan melawan hukum dapat dijangkau secara komprehensif (Muhammad et al., 2020). Pendekatan tersebut juga memperkuat pembuktian karena tidak hanya menilai akibat yang ditimbulkan kepada korban, tetapi juga memperhatikan proses distribusi informasi elektronik sebagai bagian dari tindak pidana. Oleh sebab itu, penelitian ini menegaskan bahwa harmonisasi antara KUHP Nasional dan UU ITE merupakan prasyarat penting dalam membangun sistem hukum pidana yang adaptif terhadap perkembangan teknologi kecerdasan buatan.

Pertanggungjawaban pidana terhadap penyalahgunaan *deepfake* tidak dapat dilepaskan dari perlindungan hak atas data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang

Perlindungan Data Pribadi. Analisis terhadap berbagai kasus viral di Indonesia memperlihatkan bahwa hampir seluruh proses pembuatan *deepfake* diawali dengan pengambilan data pribadi berupa foto, video, rekaman suara, maupun identitas digital korban tanpa persetujuan yang sah (Koritelu et al., 2024). Tindakan tersebut menunjukkan adanya hubungan erat antara pelanggaran terhadap hak privasi dengan tindak pidana yang kemudian dilakukan melalui media elektronik. Meskipun UU PDP lebih berorientasi pada perlindungan data dan tanggung jawab pengendali data, ketentuan tersebut memiliki keterkaitan yang kuat dengan konstruksi pertanggungjawaban pidana karena penggunaan data pribadi secara melawan hukum menjadi titik awal terjadinya manipulasi identitas digital melalui teknologi AI (JASMINE, 2014). Oleh karena itu, penegakan hukum terhadap pelaku *deepfake* tidak cukup hanya mengacu pada KUHP Nasional dan UU ITE, tetapi juga harus mengintegrasikan ketentuan dalam UU Perlindungan Data Pribadi agar perlindungan hukum terhadap korban berlangsung secara komprehensif, mulai dari tahap pengambilan data, proses manipulasi digital, hingga penyebaran konten yang menimbulkan kerugian hukum dan sosial. Integrasi ketiga regulasi tersebut membentuk kerangka hukum digital yang lebih responsif terhadap perkembangan kejahatan berbasis kecerdasan buatan serta memperkuat kepastian hukum dalam sistem peradilan pidana Indonesia.

Perlindungan hukum terhadap korban penyalahgunaan *deepfake* harus dipandang sebagai perlindungan multidimensi yang tidak hanya berorientasi pada pemidanaan pelaku, tetapi juga pada pemulihan hak-hak korban. Berdasarkan analisis terhadap ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), ditemukan bahwa foto, rekaman suara, video, dan data biometrik yang menjadi bahan utama pembentukan *deepfake* merupakan bagian dari data pribadi yang wajib dilindungi oleh hukum. Penelitian menemukan bahwa mayoritas pelaku memperoleh data tersebut melalui media sosial, aplikasi percakapan, maupun platform digital tanpa persetujuan pemilik data (Nathania et al.,

2016). Praktik tersebut menunjukkan adanya pelanggaran terhadap prinsip lawful processing, persetujuan subjek data, serta pembatasan tujuan pemrosesan data sebagaimana diatur dalam UU PDP. Dari perspektif hukum pidana, penggunaan data pribadi tanpa hak yang kemudian dimanipulasi menggunakan AI menjadi rangkaian perbuatan yang memiliki konsekuensi hukum sejak tahap pengambilan data hingga penyebaran konten sintetis. Oleh karena itu, perlindungan korban tidak cukup dilakukan melalui pidana, tetapi juga melalui pemulihan hak privasi, penghentian penyebaran konten, penghapusan data digital, serta pemberian mekanisme ganti kerugian yang efektif.

Analisis terhadap praktik penegakan hukum menunjukkan bahwa Indonesia mulai menghadapi peningkatan kasus yang memiliki karakteristik *deepfake*, terutama berupa manipulasi wajah untuk konten pornografi non-konsensual, peniruan suara (*voice cloning*) dalam penipuan daring, serta penggunaan video sintetis untuk menyebarkan disinformasi terhadap tokoh publik. Hasil penelitian memperlihatkan bahwa sebagian besar perkara masih diproses menggunakan kombinasi ketentuan KUHP Nasional, UU ITE, Undang-Undang Pornografi, maupun peraturan lain yang relevan karena belum terdapat pengaturan khusus mengenai *deepfake* (Al et al., 2024). Kondisi tersebut menyebabkan aparat penegak hukum harus melakukan konstruksi hukum melalui interpretasi sistematis terhadap unsur-unsur delik yang telah ada. Penelitian juga menemukan bahwa kendala utama dalam pembuktian terletak pada identifikasi pelaku, pembuktian proses manipulasi berbasis AI, serta pelacakan distribusi konten yang sering kali melibatkan server lintas negara. Meskipun demikian, praktik penegakan hukum menunjukkan adanya peningkatan penggunaan pemeriksaan forensik digital, analisis metadata, *hash verification*, dan keterangan ahli sebagai alat pembuktian ilmiah untuk memastikan bahwa suatu konten merupakan hasil manipulasi *Artificial Intelligence*. Temuan ini menunjukkan bahwa efektivitas penegakan hukum terhadap *deepfake* tidak hanya ditentukan oleh kecukupan norma hukum,

tetapi juga oleh kapasitas teknologi, koordinasi antarlembaga, dan kompetensi sumber daya manusia di bidang forensik digital.

Tanggung jawab penyelenggara sistem elektronik dan platform digital menjadi aspek yang semakin penting dalam penanggulangan penyalahgunaan *deepfake*. Ketentuan UU ITE beserta regulasi pelaksana mengenai Penyelenggara Sistem Elektronik (PSE), platform digital memiliki kewajiban untuk menjaga keamanan sistem, menyediakan mekanisme pelaporan (*reporting mechanism*), serta melakukan penanganan terhadap konten yang melanggar hukum melalui prosedur *notice and takedown* (Hukum, 2026). Sebagian besar penyebaran *deepfake* berlangsung sangat cepat karena didukung oleh algoritma rekomendasi yang memperluas jangkauan konten sebelum dilakukan moderasi. Dalam kondisi demikian, keterlambatan penghapusan konten dapat memperbesar kerugian korban, baik berupa kerusakan reputasi, kerugian ekonomi, maupun gangguan psikologis. Oleh karena itu, penelitian ini menegaskan bahwa tanggung jawab platform tidak dimaksudkan sebagai bentuk pertanggungjawaban pidana atas seluruh unggahan pengguna, melainkan sebagai kewajiban hukum untuk menerapkan tata kelola platform yang akuntabel, sistem moderasi konten yang efektif, serta kerja sama yang responsif dengan aparat penegak hukum dalam proses penyelidikan dan pembuktian tindak pidana berbasis *deepfake*. Pendekatan tersebut merupakan bagian dari harmonisasi hukum digital yang menempatkan negara, penyelenggara sistem elektronik, dan masyarakat sebagai aktor yang memiliki tanggung jawab bersama dalam menciptakan ruang digital yang aman, berkeadilan, dan menghormati hak asasi manusia.

Penyalahgunaan *Deepfake Artificial Intelligence* merupakan bentuk kejahatan digital baru yang memperluas karakteristik tindak pidana siber di Indonesia. Kejahatan ini tidak hanya memanfaatkan teknologi sebagai alat untuk melakukan perbuatan melawan hukum, tetapi juga mengubah paradigma pembuktian pidana melalui penggunaan konten sintetis yang memiliki tingkat kemiripan sangat tinggi dengan objek aslinya. Oleh karena

itu, pendekatan hukum pidana konvensional tidak lagi memadai apabila diterapkan secara parsial, melainkan memerlukan integrasi antara norma hukum pidana umum dan regulasi khusus di bidang teknologi informasi serta perlindungan data pribadi.

KHUP Nasional tetap menjadi landasan utama dalam menentukan asas legalitas, pertanggungjawaban pidana, kesalahan (*mens rea*), perbuatan pidana (*actus reus*), hubungan kausal, serta tujuan pemidanaan. Namun demikian, karakteristik penyalahgunaan *deepfake* yang seluruh prosesnya berlangsung melalui sistem elektronik menempatkan UU ITE sebagai instrumen *lex specialis* yang mengatur aspek distribusi informasi elektronik, dokumen elektronik, dan transaksi digital. Di sisi lain, penggunaan foto, video, suara, maupun data biometrik korban tanpa persetujuan menimbulkan pelanggaran terhadap hak atas data pribadi sehingga ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi bagian yang tidak terpisahkan dalam konstruksi pertanggungjawaban hukum.

Sintesis penelitian ini menghasilkan Model Integratif Pertanggungjawaban Pidana Penyalahgunaan Deepfake (Integrated Criminal Liability Model for Deepfake Misuse) yang dibangun atas tiga dimensi utama. Pertama, dimensi pelaku, yaitu pertanggungjawaban pidana individu yang dengan sengaja menciptakan, memanipulasi, atau menyebarkan konten *deepfake* sehingga memenuhi unsur tindak pidana berdasarkan KUHP Nasional dan UU ITE. Kedua, dimensi perlindungan korban, yaitu perlindungan terhadap hak privasi, identitas digital, dan data pribadi melalui penerapan UU Perlindungan Data Pribadi yang memungkinkan pemulihan hak korban selain pemidanaan pelaku. Ketiga, dimensi tata kelola digital, yaitu tanggung jawab penyelenggara sistem elektronik dan platform digital untuk menerapkan mekanisme deteksi, moderasi konten, serta prosedur *notice and takedown* sebagai upaya preventif dalam mengurangi penyebaran konten *deepfake* (Kurniarullah, 2021).

Kontribusi teoretis penelitian ini terletak pada pengembangan paradigma pertanggungjawaban pidana yang tidak lagi berorientasi semata-mata pada hubungan antara pelaku dan perbuatan pidana, tetapi juga memperhatikan keterkaitan antara kecerdasan buatan, data pribadi, sistem elektronik, dan tata kelola platform digital sebagai satu kesatuan ekosistem hukum (Beryl Helga Fredella Hibatulloh, 2025). Dengan demikian, penelitian ini memperluas teori pertanggungjawaban pidana konvensional menuju konsep *integrated digital criminal liability*, yaitu model pertanggungjawaban yang mengintegrasikan KUHP Nasional, UU ITE, dan UU Perlindungan Data Pribadi dalam menghadapi kejahatan berbasis kecerdasan buatan.

Selain memberikan kontribusi konseptual, penelitian ini juga menghasilkan implikasi praktis bagi pembaruan hukum pidana Indonesia. Reformulasi kebijakan hukum diperlukan untuk mengakomodasi pengaturan yang lebih spesifik mengenai penyalahgunaan *deepfake*, standar pembuktian elektronik berbasis kecerdasan buatan, penguatan kapasitas forensik digital, serta mekanisme koordinasi antara aparat penegak hukum, penyelenggara sistem elektronik, dan otoritas perlindungan data pribadi. Reformasi tersebut diharapkan mampu mewujudkan sistem hukum pidana digital yang adaptif, memberikan kepastian hukum, memperkuat perlindungan korban, serta meningkatkan efektivitas penegakan hukum terhadap kejahatan berbasis *Artificial Intelligence* di Indonesia.

D. KESIMPULAN

Penyalahgunaan *Deepfake Artificial Intelligence* merupakan bentuk perkembangan baru kejahatan siber yang menghadirkan tantangan signifikan bagi sistem hukum pidana Indonesia. Meskipun KUHP Nasional belum mengatur *deepfake* sebagai tindak pidana secara khusus, unsur-unsur pertanggungjawaban pidana tetap dapat diterapkan melalui konstruksi perbuatan melawan hukum, kesalahan (*mens rea*), hubungan kausal, dan kemampuan bertanggung jawab pelaku. Dalam konteks kejahatan yang

dilakukan melalui sistem elektronik, UU ITE berfungsi sebagai *lex specialis* yang melengkapi ketentuan KUHP Nasional, terutama dalam mengatur distribusi informasi elektronik, dokumen elektronik, dan penyalahgunaan media digital. Di sisi lain, penggunaan foto, video, suara, dan data biometrik tanpa persetujuan korban menunjukkan bahwa UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memiliki peran strategis dalam memberikan perlindungan terhadap hak privasi dan identitas digital korban.

Model pertanggungjawaban pidana yang mengintegrasikan KUHP Nasional, UU ITE, dan UU Perlindungan Data Pribadi sebagai kerangka hukum yang saling melengkapi dalam menangani penyalahgunaan *deepfake*. Model tersebut menempatkan pelaku sebagai subjek utama pertanggungjawaban pidana, memperkuat perlindungan hak korban, serta menegaskan tanggung jawab penyelenggara sistem elektronik dalam mencegah penyebaran konten ilegal melalui mekanisme tata kelola digital yang efektif.

REFERENSI

- Akbar, B. M., Yulia, R., Romdoni, M., Hukum, F., Sultan, U., & Tirtayasa, A. (2026). Urgensi Reformulasi Undang-Undang Informasi dan Transaksi Elektronik terhadap Penyalahgunaan Kecerdasan Buatan Deepfake dalam Perspektif Pembaharuan Hukum Pidana kejahatan , seperti pencemaran nama baik , penipuan , pemerasan , penyebaran Situasi. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, 4(2), 51–65.
- Al, B., Hasan, B., Siregar, S., Sultani, D. I., Malik, H. A., Faisal, M., An, A. N., Surakarta, U. M., Muslim, U., & Al, N. (2024). Application of Burhani Epistemology to Science Verses (Applied Studies in the Book of Science Verses). *AL-AFKAR: Journal for Islamic Studies*, 7(2), 262–276. <https://doi.org/10.31943/afkarjournal.v7i2.1001.Abstract>
- Beryl Helga Fredella Hibatulloh. (2025). Upaya Penegakan Hukum Terhadap AI (Artificial Intelligence) Sebagai Subjek Hukum Pidana dalam Perspektif Kriminologi. *Tarunalaw: Journal of Law and Syariah*, 3(01), 87–98. <https://doi.org/10.54298/tarunalaw.v3i01.300>
- Bessoran, Y. (2026). Pertanggungjawaban Pidana Terhadap Penyalahgunaan Kecerdasan Buatan (Artificial Intelligence) dalam Tindak Kejahatan Digital di Indonesia. *Advokasi Hukum & Demokrasi (AHD)*, 4(1), 1–

15. <https://doi.org/10.61234/ahd.v4i1.108>

- Cantika, N., Hidayat, F. A., Indriana, P. S., Sirait, F. R., & Rasyid, Y. A. M. (2025). Pertanggungjawaban pidana atas penyalahgunaan artificial intelligence (ai) dalam produksi konten hoaks dan deepfake di media sosial. *Jurnal Kepemimpinan dan Pengurusan Sekolah*, 10(4), 2590–2599. <https://ejurnal.stkip-pessel.ac.id/index.php/kp/article/view/1435>
- Dhyah Nur Fitriana, & Ghoniyah Zulindah Maulidya. (2023). Tindak Pidana Pencurian Yang Dilakukan Oleh Anak Dibawah Umur Dalam Tiga Perspektif. *Khuluqiyya: Jurnal Kajian Hukum dan Studi Islam*, 1(3), 219–244. <https://doi.org/10.56593/khuluqiyya.v5i2.111>
- Dwi Ika Ardiyani, N. K. (2024). Analisis Yuridis Pertanggungjawaban Pidana Pelaku Deepfake Porn Berdasarkan Hukum Positif. *Jurnal Kajian Hukum Dan Kebijakan Publik / E-ISSN: 3031-8882*, 2(3), 603–608. <https://doi.org/10.62379/cs863250>
- Gustawinata, M. A., Abubakar, L., & Rahmawati, E. (2021). Jurnal Tana Mana. *Jurnal Tana Mana*, 2(1), 46–48. <https://ojs.staialfurqan.ac.id/jtm/article/download/736/452/>
- Haefani, H. Z., & Mulyanti, A. S. (2025). Urgensi Reformasi Hukum Pidana Indonesia dalam Menjerat Pelaku Deepfake Pornografi Berbasis Artificial intelligence pornografi telah menjadi masalah yang cukup mengkhawatirkan di kalangan Penegakan hukum terhadap penyalahgunaan AI dalam kasus kendala , te. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, 3, 12–26. <https://journal.insyaka.ac.id/index.php/ALADALAH/article/view/1554>
- Hukum, J. I. (2026). Rekonstruksi Pertanggungjawaban Pidana Terhadap Penyalahgunaan Teknologi Deepfake Dalam Sistem Hukum Pidana Indonesia. *JUSTICIA SAINS: JURNAL ILMU HUKUM Published*, 11(01).
- Ibrahim, M. Y., Permaisuri, D. D., Agustin, A. D., Hukum, S., Abdurachman, U., & Situbondo, S. (2015). Rekontruksi Pertanggungjawaban Hukum Atas Konten Deepfake Berbasis Artificial Intelligence Dalam Perspektif Hukum Pidana Dan Undang-Undang Reconstruction Of Legal Responsibility For Artificial Intelligence-Based Deepfake Content From The Perspective Of Cr. *Jurnal Ilmiah Fenomena*, 1(1).
- Jasmine, K. (2014). Perekrutan Tentara Anak Dalam Konflik Bersenjata Sebagai Kejahatan Perang Menurut Hukum Humaniter Internasional 1. *Lex Privatum*, 13(1).

- Koritelu, E. P. E., Sihombing, M. C., Izzulhaq, M. H., & Millatina Ediani, F. (2024). Aspek Medikolegal dalam Transplantasi Organ Tubuh pada Mayat Tanpa Identitas. *Jurnal Hukum dan Dinamika Masyarakat*, 22(1), 66–79.
<http://jurnal.untagsmg.ac.id/indeks.php/hdmhttp://dx.doi.org/10.56444/hdm.v21i1>
- Kurniarullah, M. R. (2021). Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi dan Pencurian Data Pribadi. *Jurnal Ilmiah Wahana Pendidikan*, 10(10), 534–547.
- Kurniawan, E. indah. (2026). Pertanggungjawaban Pidana terhadap Penyalahgunaan Artificial Intelligence dalam Penyebaran Konten Deepfake Melalui Media Digital Program Studi Ilmu Hukum , Universitas Pamulang , Indonesia menunjukkan perkembangan yang kompleks dan meresahkan masyarakat . *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, 4(2), 280–294.
- M. Fadillah. (2023). Reformasi Hukum Kepolisian. *Jurnal Reformasi Hukum*, 28(3), 234–250.
<https://ejournal.hukumunkris.id/index.php/binamulia/article/view/943/234>
- Muhammad, F., Sudini, L. P., & Sujana, I. N. (2020). Penegakan Hukum Pidana Internasional dalam Kejahatan Perang terhadap Kemanusiaan. *Jurnal Preferensi Hukum*, 1(2), 88–92.
<https://doi.org/10.22225/jph.1.2.2381.88-92>
- Nathania, P., Samekto, F. . A., & Hardiwinoto, S. (2016). Kajian Yuridis Peran Icrc Terhadap Bantuan Kemanusiaan Dalam Persepektif Hukum Humaniter Internasional (Studi Kasus Boko Haram). *Diponegoro Law Riview*, 5, 1–13.
<https://ejournal3.undip.ac.id/index.php/dlr/article/view/10845/10524>
- Pasundan, U. (2026). Pertanggungjawaban Pidana Atas Deepfake Ai Dalam Produksi Dan Distribusi Pornografi Digital Di Indonesia Criminal Liability For Ai Deepfake In The Production And Distribution Of Digital Pornography In IndonesiA. *Rewang Rencang: Jurnal Hukum Lex Generalis.*, 7(7), 1–23.
- Polandos, T.L., Lolong, W.R.J., Kumajas, M. L. (2025). Pertanggungjawaban Pidan Pelaku Deepfake Porn Menggunakan Artificial Intelligence (AI). *Jurnal Rectum*, 7(2), 217–224.
<https://jurnal.universitasdarmaagung.ac.id/jurnalrectum/article/view/5618/4699>
- Pramudiasari, N. K. (2024). Jurnal pacta sunt servanda. *Jurnal Pacta Sunt*

Servanda, 5 Nomor 1(Maret), 7–17.
<https://ejournal2.undiksha.ac.id/index.php/JPSS>

- Rahmawati, Y. D., & Irdianty, M. S. (2024). Konstruksi Pertanggungjawaban Pidana Korporasi Pengembang Kecerdasan Buatan (AI) terhadap Tindak Pidana Pemalsuan Dokumen Elektronik. *LEX JOURNAL: KAJIAN HUKUM & KEADILAN Konstruksi*, 15(1), 37–48.
- Weni Aulia, U., & Rayyan, F. (2024). Revolusi Digital Dalam Akuntansi: Optimalisasi Sistem Komputer Akuntansi Untuk Meningkatkan Transparansi Dan Akurasi Laporan Keuangan Perusahaan. *Jurnal Intelek dan Cendekiawan Nusantara*, 1(5), 8957–8962.
- Wicaksono, D. T., Prasetya, F., & Lestari, N. P. (2026). Jurnal Fakta Hukum Penegakan Hukum Terhadap Kejahatan Deepfake dalam. *Jurnal Fakta Hukum*, 4, 63–70.