SIMPUL: Jurnal Ilmu Politik dan Hukum
Vol. 2, No. 2, Juni 2026, pp. 38-48
eISSN 3090-0867 | https://ejournal.gemacendekia.org/index.php/simpul

Pertanggungjawaban Pidana atas Penyalahgunaan AI Generatif: Celah Hukum dalam KUHP Baru dan UU ITE

Mahmud [a,1*], Nurfaidah [b,2]

[a] Program Studi Hukum Tata Negara, Fakultas Hukum, Universitas Islam Indonesia, Yogyakarta
[b] Program Studi Ilmu Pemerintahan, Sekolah Tinggi Pembangunan Masyarakat Desa "APMD" Yogyakarta, Indonesia
[1] mahmudyana97@gmail.com *; [2] nurfaidahpertama@gmail.com
* Corresponding Author

ABSTRACT

The rapid development of generative artificial intelligence (AI) technology has brought significant changes to various aspects of life, including the field of criminal law. On the one hand, this technology offers great benefits in terms of efficiency and innovation; on the other hand, it also opens the door to various new forms of crime, such as the creation of deepfake content, the spread of disinformation, and fraud based on digital impersonation. Problems arise when the existing legal framework, particularly in the new Criminal Code and the Law on Information and Electronic Transactions (ITE Law), does not explicitly regulate the misuse of generative AI. This creates a legal loophole in determining the form of criminal liability, especially regarding the element of fault (mens rea) and the legal subjects that can be held liable. This study aims to analyze the concept of criminal liability for the misuse of generative AI and to identify legal loopholes in the new Criminal Code and the UU ITE. The method used was normative legal research employing a legislative and conceptual approach, supported by primary and secondary legal sources. The findings indicate that while certain provisions in the new Criminal Code and the ITE Law can be used to prosecute perpetrators, there remain limitations in addressing the complexity of AI-based crimes, particularly regarding the burden of proof, attribution of acts, and the determination of liable parties. A reformulation of the law is needed that is more adaptive to technological developments, including specific regulations regarding generative AI as well as adjustments to the concept of criminal liability so as to provide legal certainty and effective protection for the public.

Article History
Received 2026-06-11
Revised 2026-06-19
Accepted 2026-06-19
Published 2026-06-30

Keywords
Generative AI, Criminal Liability, Legal Loopholes, New Criminal Code, ITE Law.

Copyright © 2025, The Author(s)
This is an open-access article under the CC–BY-SA license

1. Pendahuluan

Perkembangan teknologi digital telah memasuki fase yang semakin kompleks dengan hadirnya artificial intelligence (AI), khususnya AI generatif, yang mampu menghasilkan konten baru secara otomatis seperti teks, gambar, audio, dan video. Teknologi ini menjadi salah satu inovasi paling signifikan dalam era transformasi digital karena kemampuannya meniru bahkan melampaui kreativitas manusia dalam menghasilkan konten. Namun demikian, kemajuan tersebut tidak hanya membawa manfaat, tetapi juga memunculkan risiko baru dalam bentuk penyalahgunaan teknologi yang berpotensi menimbulkan dampak hukum serius, khususnya dalam ranah hukum pidana.

AI generatif memiliki karakteristik utama berupa kemampuannya menciptakan konten yang sangat realistis dan sulit dibedakan dari kenyataan. Salah satu manifestasi paling nyata adalah teknologi deepfake, yaitu teknik manipulasi berbasis AI yang dapat mengubah wajah, suara, atau ekspresi seseorang dalam suatu media digital sehingga tampak autentik. Fenomena ini telah berkembang pesat dan digunakan dalam berbagai konteks, baik yang bersifat positif maupun negatif. Dalam konteks negatif, deepfake sering dimanfaatkan untuk tujuan kriminal seperti penipuan, pencemaran nama baik, hingga pembuatan konten pornografi tanpa persetujuan korban (Prayoga & Edrisy, 2025).

Penyalahgunaan AI generatif telah menciptakan pola kejahatan baru yang sebelumnya tidak dikenal dalam hukum pidana konvensional. Teknologi ini dapat digunakan untuk

melakukan impersonasi digital dengan meniru identitas seseorang secara visual maupun audio, sehingga mempermudah pelaku dalam melakukan penipuan atau manipulasi informasi. Selain itu, AI generatif juga memungkinkan produksi dan penyebaran disinformasi secara masif dan sistematis, yang dapat mempengaruhi opini publik serta mengganggu stabilitas sosial dan politik. Bahkan, dalam beberapa kasus, penggunaan deepfake telah menyebabkan pelanggaran serius terhadap privasi dan martabat individu, terutama melalui konten pornografi non-konsensual (Dian Ningtias et al, 2025).

Dalam konteks Indonesia, perkembangan teknologi ini belum sepenuhnya diimbangi dengan kesiapan regulasi hukum yang memadai. Saat ini, pengaturan mengenai kejahatan berbasis teknologi informasi masih bertumpu pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP) yang baru disahkan melalui Undang-Undang Nomor 1 Tahun 2023. Namun, kedua instrumen hukum tersebut belum secara eksplisit mengatur mengenai penyalahgunaan AI generatif. Hal ini menimbulkan kekosongan norma atau setidaknya ketidakjelasan pengaturan yang berpotensi menghambat penegakan hukum.

Dalam UU ITE, fokus pengaturan lebih diarahkan pada konten dan aktivitas dalam sistem elektronik, seperti penyebaran informasi yang melanggar hukum. Akan tetapi, UU ITE belum secara spesifik mengantisipasi teknologi yang digunakan untuk menghasilkan konten tersebut, termasuk AI generatif. Akibatnya, ketika terjadi kejahatan berbasis AI seperti deepfake, aparat penegak hukum seringkali harus menggunakan pendekatan interpretasi terhadap pasal-pasal yang ada, yang belum tentu mampu menjangkau kompleksitas permasalahan secara menyeluruh. Regulasi terkait AI di Indonesia masih bersifat umum dan belum mampu mengatur secara spesifik aspek teknis maupun operasional dari teknologi tersebut (Arlando Israel Kamasi et al, 2026).

Sementara itu, KUHP baru sebagai bentuk pembaruan hukum pidana nasional juga belum memberikan perhatian khusus terhadap perkembangan AI. Meskipun KUHP 2023 telah membawa sejumlah pembaruan penting, seperti pengakuan terhadap hukum yang hidup dalam masyarakat dan perluasan subjek hukum, namun pengaturan mengenai kejahatan berbasis AI masih bersifat implisit. Tidak adanya ketentuan yang secara tegas mengatur tindak pidana berbasis AI, termasuk pemalsuan identitas atau manipulasi konten digital, menunjukkan adanya celah hukum yang signifikan. KUHP 2023 belum secara tersurat mengatur tindak pidana berbasis AI, sehingga perlindungan hukum terhadap korban menjadi kurang optimal (Azzahra & Lukitasari, 2025).

Lebih juah, baik KUHP maupun UU ITE belum mampu mengakomodasi fenomena deepfake secara komprehensif. Ketiadaan norma yang secara eksplisit mengatur teknologi ini menyebabkan kesulitan dalam mengkualifikasikan perbuatan sebagai tindak pidana serta dalam menentukan unsur-unsur delik yang relevan. Bahkan, dalam kasus tertentu seperti deepfake pornography, ketentuan hukum yang ada dinilai tidak memadai karena tidak memasukkan manipulasi berbasis AI sebagai bagian dari unsur tindak pidana, sehingga pelaku sulit dimintai pertanggungjawaban pidana (Muhammad Afif, 2025).

Permasalahan menjadi semakin kompleks ketika dikaitkan dengan konsep pertanggungjawaban pidana. Dalam hukum pidana klasik, pertanggungjawaban didasarkan pada adanya kesalahan (mens rea) dan perbuatan (actus reus) yang dilakukan oleh subjek hukum tertentu. Namun, dalam konteks AI generatif, terdapat kerancuan mengenai siapa yang sebenarnya bertanggung jawab atas suatu perbuatan yang melibatkan teknologi tersebut. Apakah tanggung jawab berada pada pengguna yang mengoperasikan AI, pengembang yang menciptakan sistem, atau penyedia platform yang mendistribusikan teknologi tersebut? Pertanyaan ini menunjukkan bahwa konsep pertanggungjawaban pidana yang ada saat ini belum sepenuhnya mampu menjawab tantangan yang ditimbulkan oleh AI.

Selain itu, aspek pembuktian dalam hukum pidana juga menghadapi permasalahan serius akibat perkembangan AI generatif. Konten yang dihasilkan oleh teknologi ini seringkali sangat sulit dibedakan dari konten asli, sehingga menyulitkan proses verifikasi dalam pembuktian di pengadilan. Hal ini berpotensi menimbulkan ketidakpastian hukum dan bahkan membuka peluang terjadinya kesalahan dalam penegakan hukum. Oleh karena itu, diperlukan pendekatan baru yang tidak hanya mengandalkan metode pembuktian konvensional, tetapi juga memanfaatkan teknologi forensik digital yang lebih canggih.

Berbagai negara telah mulai merespons permasalahan ini dengan mengembangkan regulasi khusus terkait AI. Beberapa negara telah mengatur secara spesifik penggunaan deepfake dan menetapkan sanksi pidana terhadap penyalahgunaannya. Indonesia masih tertinggal dalam pengaturan AI dibandingkan dengan negara lain yang telah memiliki instrumen hukum yang lebih adaptif terhadap perkembangan teknologi (Ramadan & Wahyudi, 2025). Oleh karena itu, reformulasi hukum menjadi kebutuhan yang mendesak untuk memastikan bahwa sistem hukum nasional mampu menghadapi dinamika teknologi yang terus berkembang.

Terdapat kesenjangan yang signifikan antara perkembangan teknologi AI generatif dengan kerangka hukum yang berlaku di Indonesia. Ketiadaan pengaturan yang spesifik dalam KUHP baru dan UU ITE menciptakan celah hukum yang berpotensi dimanfaatkan oleh pelaku kejahatan. Oleh karena itu, diperlukan kajian mendalam mengenai pertanggungjawaban pidana atas penyalahgunaan AI generatif serta upaya reformulasi hukum yang lebih adaptif dan responsif terhadap perkembangan teknologi. Kajian ini menjadi penting tidak hanya untuk memberikan kepastian hukum, tetapi juga untuk melindungi masyarakat dari dampak negatif penggunaan teknologi yang tidak bertanggung jawab.

2. Metode Penelitian

Penelitian ini menggunakan jenis penelitian yuridis normatif, yaitu penelitian yang berfokus pada analisis norma hukum yang berlaku terkait pertanggungjawaban pidana atas penyalahgunaan AI generatif. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dengan menelaah ketentuan dalam Undang-Undang Nomor 1 Tahun 2023 tentang KUHP dan Undang-Undang Informasi dan Transaksi Elektronik, serta pendekatan konseptual (*conceptual approach*) yang mengkaji doktrin hukum pidana, khususnya terkait konsep kesalahan (*mens rea*) dan pertanggungjawaban pidana. Bahan hukum yang digunakan terdiri dari bahan hukum primer berupa peraturan perundang-undangan, serta bahan hukum sekunder seperti buku, jurnal ilmiah, dan hasil penelitian yang relevan dengan permasalahan AI generatif dan hukum pidana. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*), sedangkan analisis dilakukan secara kualitatif dengan metode deskriptif-analitis guna mengidentifikasi celah hukum dan merumuskan argumentasi hukum yang komprehensif.

3. Hasil dan Pembahasan

Penyalahgunaan AI Generatif

Perkembangan artificial intelligence (AI) generatif telah membawa perubahan signifikan dalam lanskap kejahatan modern. Teknologi ini memungkinkan penciptaan konten digital yang sangat realistis melalui proses otomatis berbasis algoritma pembelajaran mesin. Dalam perspektif hukum pidana, AI generatif tidak hanya berfungsi sebagai alat bantu teknologi, tetapi juga telah menjadi medium baru yang memfasilitasi lahirnya berbagai bentuk tindak pidana dengan karakteristik yang lebih kompleks dan sulit diidentifikasi. Hal ini menimbulkan tantangan serius bagi sistem hukum, terutama dalam mengkualifikasikan perbuatan dan menentukan pertanggungjawaban pidana.

Bentuk-bentuk penyalahgunaan AI generatif. Pertama, penggunaan teknologi deepfake. Deepfake merupakan hasil rekayasa AI yang mampu memanipulasi wajah, suara, maupun gerakan seseorang sehingga tampak autentik. Teknologi ini dirancang agar konten yang dihasilkan "dipersepsikan sebagai nyata" oleh publik (Diel et al, 2025). Dalam praktiknya, deepfake sering digunakan untuk membuat video palsu yang dapat menyesatkan, merusak reputasi, atau bahkan menipu korban. Dalam hukum pidana, tindakan ini dapat dikualifikasikan sebagai pencemaran nama baik, penipuan, maupun penyebaran informasi palsu, tergantung pada tujuan dan akibat yang ditimbulkan.

Kedua, deepfake sering digunakan dalam kejahatan berbasis identitas digital. Teknologi ini memungkinkan pelaku untuk meniru identitas seseorang secara visual maupun audio, sehingga dapat digunakan dalam modus impersonasi digital. Deepfake telah menjadi sarana dalam penipuan identitas digital karena kemampuannya menghasilkan konten yang sulit dibedakan dari aslinya (Firdaus & Puspita, 2025). Dalam konteks hukum pidana, impersonasi

ini dapat dikualifikasikan sebagai penipuan atau pemalsuan identitas, terutama jika digunakan untuk memperoleh keuntungan secara melawan hukum. Bahkan deepfake telah digunakan dalam skema penipuan keuangan yang kompleks, menunjukkan risiko kejahatan berbasis AI.

Ketiga, pembuatan dan penyebaran konten pornografi non-konsensual (*non-consensual deepfake pornography*). Dalam kasus ini, wajah seseorang ditempelkan pada tubuh dalam konten pornografi tanpa persetujuan yang bersangkutan. Praktik ini merupakan salah satu bentuk kejahatan yang paling merugikan korban karena tidak hanya melanggar privasi, tetapi juga merusak martabat dan integritas individu. Deepfake sering digunakan untuk memanipulasi wajah seseorang dalam video pornografi tanpa izin, bahkan untuk tujuan eksploitasi atau keuntungan tertentu (Chairani & Pradhana, 2024). Dalam perspektif hukum pidana, perbuatan ini dapat dikualifikasikan sebagai tindak pidana kesusilaan, pelanggaran privasi, atau bahkan kekerasan berbasis gender dalam ruang digital.

Keempat, AI generatif berperan dalam penyebaran disinformasi dan hoaks secara masif. Dengan kemampuan menghasilkan teks, gambar, dan video secara otomatis, pelaku dapat menciptakan narasi palsu yang tampak kredibel dan menyebarkannya dalam skala besar. Fenomena ini menjadi ancaman serius karena dapat mempengaruhi opini publik dan merusak kepercayaan terhadap informasi digital. Deepfake dan konten sintetis memiliki dampak signifikan terhadap perilaku dan persepsi manusia, termasuk dalam membentuk keyakinan terhadap informasi yang salah (Diel et al, 2025). Dalam hukum pidana, tindakan ini dapat dikategorikan sebagai penyebaran berita bohong atau informasi menyesatkan yang merugikan kepentingan umum.

Kelima, AI generatif digunakan dalam tindak pidana penipuan berbasis rekayasa sosial (*social engineering*). Dengan memanfaatkan kemampuan AI dalam meniru gaya komunikasi manusia, pelaku dapat membuat pesan atau percakapan yang tampak autentik untuk memanipulasi korban. Dalam beberapa kasus, pelaku bahkan menggunakan suara sintetis untuk meniru suara orang tertentu guna meyakinkan korban. Hal ini menunjukkan bahwa AI generatif tidak hanya digunakan untuk manipulasi visual, tetapi juga audio, yang semakin memperluas spektrum kejahatan. Kejahatan berbasis AI, termasuk deepfake fraud, menjadi tantangan serius bagi penegak hukum karena kompleksitasnya yang tinggi (Lin, 2025).

Keenam, AI generatif dapat dimanfaatkan untuk mendukung tindak pidana pemalsuan dokumen. Teknologi ini memungkinkan pembuatan dokumen digital yang tampak autentik, seperti surat resmi, identitas, atau kontrak, yang kemudian digunakan untuk menipu korban atau pihak berwenang. Dalam hukum pidana, tindakan ini termasuk dalam kategori pemalsuan, namun penggunaan AI sebagai alat memperumit proses pembuktian karena sulitnya membedakan antara dokumen asli dan hasil rekayasa.

Ketuju, penyalahgunaan AI generatif berpotensi mengganggu sistem peradilan pidana itu sendiri. Salah satu tantangan utama adalah kesulitan dalam mendeteksi keaslian bukti digital. Manusia tidak selalu mampu membedakan antara konten asli dan deepfake secara akurat, sehingga meningkatkan risiko kesalahan dalam proses pembuktian (Mai et al, 2023). Hal ini dapat berdampak serius terhadap prinsip keadilan, karena bukti yang digunakan dalam persidangan dapat diragukan keabsahannya.

Dari perspektif hukum pidana, berbagai bentuk penyalahgunaan AI generatif tersebut pada dasarnya masih dapat dijangkau melalui norma yang ada, seperti ketentuan mengenai penipuan, pencemaran nama baik, pornografi, dan penyebaran berita bohong. Namun, pendekatan ini memiliki keterbatasan karena hukum pidana yang ada belum secara spesifik dirancang untuk menghadapi teknologi AI. Akibatnya, sering terjadi kesulitan dalam mengkualifikasikan perbuatan, membuktikan unsur kesalahan, serta menentukan subjek yang bertanggung jawab.

Kejahatan berbasis AI, khususnya deepfake, menuntut adanya reformulasi konsep pertanggungjawaban pidana. Hal ini karena AI tidak hanya berfungsi sebagai alat pasif, tetapi juga dapat beroperasi secara semi-otonom dalam menghasilkan konten (Wafi et al, 2025). Kondisi ini menimbulkan pertanyaan mengenai sejauh mana tanggung jawab dapat dibebankan kepada pengguna, pengembang, atau bahkan sistem AI itu sendiri.

Pertanggungjawaban Pidana

Pertanggungjawaban pidana merupakan inti dari hukum pidana yang menentukan apakah suatu perbuatan dapat dibebankan kepada subjek hukum tertentu. Dalam doktrin klasik, pertanggungjawaban pidana mensyaratkan adanya perbuatan pidana (*actus reus*) dan kesalahan (*mens rea*) yang dilakukan oleh manusia sebagai subjek hukum. Namun, perkembangan artificial intelligence (AI) generatif telah menimbulkan tantangan serius terhadap konsep tersebut, karena teknologi ini mampu menghasilkan tindakan atau output yang tidak sepenuhnya berada dalam kendali langsung manusia.

Dalam konteks penyalahgunaan AI generatif, problem utama terletak pada atribusi pertanggungjawaban, yaitu siapa yang harus bertanggung jawab atas suatu akibat hukum yang timbul. Secara umum, terdapat tiga aktor utama yang relevan, yakni pengguna (*user*), pengembang (*developer*), dan penyedia platform (*provider*). Ketiganya memiliki peran berbeda, sehingga pendekatan pertanggungjawaban pidana tidak dapat disamaratakan.

Pertama, pengguna AI merupakan subjek yang paling mudah dimintai pertanggungjawaban pidana. Hal ini karena pengguna memiliki kontrol langsung terhadap penggunaan teknologi dan tujuan dari perbuatannya. Dalam banyak kasus, penyalahgunaan AI generatif—seperti pembuatan deepfake untuk penipuan atau pencemaran nama baik—dilakukan secara sadar oleh pengguna. Oleh karena itu, unsur *mens rea* dapat terpenuhi apabila terdapat kesengajaan (*dolus*) atau bahkan kelalaian (*culpa*) dalam penggunaan teknologi tersebut. Dalam perspektif ini, AI diposisikan sebagai alat (*tool*) yang digunakan oleh pelaku manusia, sehingga pertanggungjawaban tetap bersifat antropocentris.

Namun demikian, persoalan muncul ketika AI generatif menghasilkan output yang tidak sepenuhnya dapat diprediksi oleh pengguna. Sistem AI berbasis *self-learning algorithm* memiliki kemampuan untuk menghasilkan konten secara otonom berdasarkan data pelatihan yang kompleks. Kondisi ini menimbulkan keraguan apakah pengguna dapat dianggap memiliki niat jahat terhadap seluruh akibat yang ditimbulkan. Perkembangan AI telah menciptakan situasi di mana akibat dapat terjadi tanpa adanya kesadaran atau kehendak manusia secara langsung, sehingga menantang konsep *mens rea* dalam hukum pidana klasik (Aprianti & Jamba, 2026).

Kedua, pengembang AI (*developer*) menjadi subjek yang relevan dalam analisis pertanggungjawaban pidana. Pengembang bertanggung jawab atas desain, pelatihan, dan implementasi sistem AI. Dalam kondisi tertentu, pengembang dapat dimintai pertanggungjawaban apabila terbukti bahwa sistem yang dibuat memiliki cacat desain atau sengaja dirancang tanpa mempertimbangkan risiko penyalahgunaan. Misalnya, apabila suatu sistem AI tidak dilengkapi dengan mekanisme pengamanan untuk mencegah produksi konten ilegal, maka dapat dikualifikasikan sebagai bentuk kelalaian.

Namun, membebankan pertanggungjawaban pidana kepada pengembang tidaklah sederhana. Hal ini karena pengembang umumnya tidak memiliki kontrol langsung terhadap penggunaan AI oleh pengguna akhir. Hukum pidana mensyaratkan adanya kesalahan individual, sehingga sulit untuk membuktikan adanya *mens rea* dari pengembang terhadap tindak pidana yang dilakukan oleh pihak lain. Oleh karena itu, pendekatan alternatif seperti *risk-based liability* atau pertanggungjawaban berbasis risiko, di mana tanggung jawab dapat dibebankan apabila terdapat kegagalan dalam mitigasi risiko teknologi (Ramadhani et al, 2025).

Ketiga, penyedia platform (*platform provider*) memiliki potensi pertanggungjawaban pidana. Platform menyediakan infrastruktur yang memungkinkan penggunaan AI generatif, serta dalam beberapa kasus memiliki kontrol terhadap distribusi konten. Dalam hukum teknologi informasi, dikenal prinsip *safe harbor*, yang menyatakan bahwa penyedia platform tidak bertanggung jawab atas konten yang dihasilkan pengguna selama mereka tidak memiliki pengetahuan atau kontrol terhadap konten tersebut. Namun, dalam konteks AI generatif, batas antara kontrol dan non-kontrol menjadi kabur, terutama ketika platform memiliki algoritma yang secara aktif memfasilitasi atau bahkan mempromosikan konten tertentu.

Dalam beberapa kasus, pertanggungjawaban dapat dibebankan kepada korporasi sebagai entitas hukum. Doktrin *corporate criminal liability* memungkinkan perusahaan pengembang atau penyedia AI untuk dimintai pertanggungjawaban apabila terbukti bahwa tindakan yang dilakukan melalui sistem AI merupakan representasi dari kehendak korporasi.

Meskipun AI bukan subjek hukum, tanggung jawab tetap dapat dialihkan kepada manusia atau badan hukum yang mengendalikan sistem tersebut (Haris & Tantimin, 2022).

Lebih kompleks lagi ketika permasalahan muncul dikaitkan dengan status AI itu sendiri. Dalam sistem hukum Indonesia saat ini, AI tidak diakui sebagai subjek hukum karena tidak memiliki kesadaran, kehendak, maupun kemampuan untuk mempertanggungjawabkan perbuatannya. Hukum pidana hanya mengenal manusia dan badan hukum sebagai subjek yang dapat dijatuhi sanksi pidana (Rahman & Habibulah, 2019). Oleh karena itu, AI tetap diposisikan sebagai alat atau agen elektronik, sehingga pertanggungjawaban harus ditelusuri kepada pihak manusia yang terlibat.

Namun demikian, perkembangan AI yang semakin otonom memunculkan wacana baru mengenai kemungkinan pemberian status hukum terbatas kepada AI. Dalam kondisi tertentu, AI dapat diperlakukan sebagai "pelaku tidak langsung" (*indirect perpetrator*) atau bahkan sebagai entitas yang memerlukan rezim pertanggungjawaban khusus. Hal ini terutama relevan dalam kasus di mana AI menghasilkan keputusan atau tindakan yang tidak dapat sepenuhnya dikontrol oleh manusia. Kerangka hukum saat ini masih mengalami kesulitan dalam menentukan posisi AI, apakah sebagai alat, perantara, atau pelaku tidak langsung dalam tindak pidana (Hutapea et al, 2026).

Selain itu, pembuktian unsur kesalahan (*mens rea*) menjadi tantangan tersendiri. Dalam hukum pidana klasik, kesalahan didasarkan pada kemampuan pelaku untuk memahami dan mengendalikan perbuatannya. Namun, dalam konteks AI generatif, terdapat fenomena *algorithmic opacity*, yaitu ketidakjelasan dalam proses pengambilan keputusan oleh sistem AI. Hal ini menyebabkan kesulitan dalam membuktikan apakah suatu akibat merupakan hasil dari niat pelaku atau konsekuensi dari sistem yang kompleks. Bahkan doktrin *mens rea* konvensional tidak lagi memadai untuk menjangkau tindakan yang dihasilkan oleh algoritma pembelajaran mandiri (Yodiansyah et al, 2026).

Lebih jauh, muncul pula konsep "responsibility gap", yaitu kesenjangan dalam pertanggungjawaban hukum akibat keterlibatan AI. Dalam situasi tertentu, tidak ada pihak yang secara jelas dapat dimintai pertanggungjawaban karena masing-masing aktor memiliki peran yang terbatas. Kondisi ini berpotensi menimbulkan ketidakadilan, baik bagi korban maupun bagi sistem hukum secara keseluruhan. Oleh karena itu, diperlukan rekonstruksi konsep pertanggungjawaban pidana yang lebih adaptif terhadap perkembangan teknologi.

KUHP baru dan UU ITE belum secara eksplisit mengatur mekanisme pertanggungjawaban pidana dalam konteks AI generatif. Akibatnya, penegakan hukum masih bergantung pada interpretasi terhadap norma yang ada, yang seringkali tidak memadai untuk menjangkau kompleksitas teknologi. Hal ini menunjukkan adanya kebutuhan mendesak untuk melakukan reformulasi hukum, baik melalui pembentukan regulasi khusus maupun melalui pengembangan doktrin hukum pidana yang lebih responsif.

Celah Hukum dalam KUHP Baru dan UU ITE

Perkembangan artificial intelligence (AI) generatif telah menciptakan tantangan baru bagi sistem hukum pidana di Indonesia, khususnya dalam konteks pengaturan dan penegakan hukum terhadap kejahatan berbasis teknologi. Meskipun Indonesia telah memiliki kerangka hukum melalui Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP baru) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), kedua instrumen tersebut belum sepenuhnya mampu menjangkau kompleksitas penyalahgunaan AI generatif. Kondisi ini menimbulkan berbagai celah hukum (*legal gaps*) yang berpotensi menghambat efektivitas penegakan hukum.

Beberapa celah hukum. Pertama, tidak adanya pengaturan eksplisit mengenai teknologi AI generatif, termasuk deepfake dan bentuk manipulasi digital lainnya. KUHP 2023 belum secara tersurat mengatur tindak pidana berbasis AI, seperti pemalsuan identitas melalui teknologi digital, sehingga perlindungan hukum terhadap korban menjadi kurang optimal (Azzahra & Lukitasari, 2025). Akibatnya, aparat penegak hukum harus mengandalkan pasal-pasal umum seperti penipuan, pemalsuan, atau pencemaran nama baik untuk menjerat pelaku.

Pendekatan ini menimbulkan masalah dalam pemenuhan unsur delik. Misalnya, dalam tindak pidana pemalsuan, terdapat unsur "membuat" yang secara tradisional merujuk pada tindakan langsung manusia. Namun dalam konteks AI generatif, konten dihasilkan melalui

proses algoritmik yang kompleks, sehingga peran manusia menjadi tidak langsung. Hal ini menimbulkan ambiguitas dalam penafsiran unsur delik dan berpotensi melemahkan konstruksi hukum pidana.

Selain itu, meskipun KUHP baru telah mencoba mengakomodasi perkembangan kejahatan siber, cakupan pengaturannya masih terbatas dan belum sepenuhnya adaptif terhadap perkembangan teknologi digital yang cepat (Fajriansyah et al, 2025). Bahkan, terdapat indikasi bahwa beberapa ketentuan dalam KUHP baru masih bersifat umum dan belum mampu menjangkau bentuk-bentuk kejahatan baru yang berbasis AI generatif.

Kedua, dalam aspek pertanggungjawaban pidana. KUHP baru belum memberikan kerangka yang jelas mengenai bagaimana pertanggungjawaban dibebankan dalam kasus yang melibatkan teknologi otonom seperti AI. Dalam praktiknya, hubungan antara pelaku dan akibat yang ditimbulkan oleh AI seringkali tidak langsung, sehingga menyulitkan pembuktian unsur kesalahan (*mens rea*). Hal ini menunjukkan bahwa konsep pertanggungjawaban pidana dalam KUHP baru masih berorientasi pada paradigma konvensional yang belum sepenuhnya relevan dengan perkembangan teknologi modern.

Di sisi lain, UU ITE sebagai lex specialis dalam bidang teknologi informasi memiliki keterbatasan yang signifikan. UU ITE lebih berfokus pada konten dan aktivitas elektronik, bukan pada teknologi yang digunakan untuk menghasilkan konten tersebut. Dengan kata lain, UU ITE mengatur "hasil" (output), tetapi belum mengatur secara memadai "proses" (proses produksi berbasis AI). Hal ini menjadi problematik dalam kasus deepfake, di mana manipulasi terjadi pada tahap produksi konten, bukan hanya pada distribusinya.

Indonesia belum memiliki ketentuan spesifik yang mengatur deepfake, sementara negara lain telah mulai mengembangkan regulasi yang lebih adaptif terhadap teknologi ini (Ramadan & Wahyudi, 2025). Ketiadaan regulasi khusus ini menyebabkan kesulitan dalam mengkualifikasikan perbuatan serta menentukan pendekatan hukum yang tepat dalam menangani kasus-kasus penyalahgunaan AI generatif.

Selain itu, terdapat tumpang tindih dan konflik normatif antara KUHP baru dan UU ITE. Studi menunjukkan bahwa perbedaan fokus dan terminologi antara kedua regulasi ini berpotensi menimbulkan ketidakpastian hukum dalam praktik penegakan hukum (Ganjar, 2025). Misalnya, suatu perbuatan dapat dijerat dengan pasal dalam KUHP maupun UU ITE secara bersamaan, sehingga menimbulkan persoalan terkait asas *lex specialis derogat legi generali* dan potensi pelanggaran asas *ne bis in idem*. Kondisi ini tidak hanya membingungkan aparat penegak hukum, tetapi juga dapat merugikan kepastian hukum bagi masyarakat.

Ketiga, berkaitan dengan atribusi pelaku dan yurisdiksi. Dalam kejahatan berbasis AI generatif, pelaku dapat beroperasi secara anonim dan lintas negara, sehingga sulit untuk diidentifikasi dan ditindak. UU ITE belum memiliki mekanisme yang memadai untuk mengatasi masalah yurisdiksi transnasional dalam konteks teknologi canggih. Hal ini semakin diperparah dengan sifat AI yang memungkinkan distribusi konten secara cepat dan luas melalui berbagai platform digital.

Selain itu, baik KUHP baru maupun UU ITE belum mengatur secara jelas mengenai tanggung jawab penyedia platform dan pengembang AI. Dalam praktiknya, platform memiliki peran penting dalam menyediakan infrastruktur dan mendistribusikan konten berbasis AI. Namun, tanpa pengaturan yang tegas, sulit untuk menentukan sejauh mana tanggung jawab dapat dibebankan kepada mereka. Kerangka hukum Indonesia masih belum mampu secara memadai mengatur kompleksitas kejahatan berbasis AI, termasuk dalam hal pembagian tanggung jawab antar actor (Fitriya et al, 2026).

Keempat, dalam aspek pembuktian digital. AI generatif mampu menghasilkan konten yang sangat realistis, sehingga sulit dibedakan dari konten asli. Hal ini menyulitkan proses pembuktian di pengadilan, terutama dalam menentukan keaslian bukti dan hubungan kausal antara perbuatan dan akibat. KUHP baru maupun UU ITE belum secara spesifik mengatur standar pembuktian untuk kasus yang melibatkan teknologi AI, sehingga berpotensi menimbulkan ketidakpastian hukum.

Reformulasi Hukum

Perkembangan pesat artificial intelligence (AI) generatif telah menimbulkan problem multidimensional bagi sistem hukum pidana Indonesia. Keterbatasan pengaturan dalam KUHP

baru dan UU ITE menunjukkan perlunya reformulasi hukum yang tidak hanya bersifat parsial, tetapi juga sistemik dan adaptif terhadap perkembangan teknologi. Reformulasi ini harus mempertimbangkan beberapa hal.

Pertama, diperlukan pembentukan regulasi khusus mengenai AI generatif yang komprehensif. Regulasi ini penting untuk mengisi kekosongan norma yang belum diatur secara eksplisit dalam KUHP baru dan UU ITE. Uni Eropa melalui *AI Act* telah mengembangkan kerangka hukum komprehensif pertama di dunia yang mengatur AI secara menyeluruh. Regulasi tersebut menegaskan bahwa hukum yang ada sebelumnya tidak cukup untuk mengatasi problem spesifik AI, sehingga diperlukan aturan khusus yang lebih adaptif (European Commission, 2026). Mengadopsi pendekatan serupa dengan merumuskan definisi AI generatif, ruang lingkup penggunaannya, serta bentuk-bentuk penyalahgunaan yang dilarang secara tegas.

Kedua, reformulasi hukum perlu mengadopsi pendekatan berbasis risiko (*risk-based approach*). Pendekatan ini terbukti efektif dalam mengklasifikasikan penggunaan AI berdasarkan tingkat bahayanya terhadap masyarakat. Dalam *AI Act*, sistem AI dibagi ke dalam beberapa kategori risiko, mulai dari risiko minimal hingga risiko tinggi dan bahkan risiko yang dilarang sepenuhnya (PwC, 2024). Semakin tinggi risiko suatu sistem AI, semakin ketat pula kewajiban hukum yang dikenakan. Pendekatan ini memungkinkan regulasi yang lebih proporsional dan fleksibel, sehingga tidak menghambat inovasi tetapi tetap memberikan perlindungan hukum yang memadai. Mengadopsi model ini untuk mengatur AI generatif, terutama dalam konteks deepfake, impersonasi digital, dan disinformasi.

Ketiga, diperlukan penyesuaian konsep pertanggungjawaban pidana agar lebih responsif terhadap karakteristik AI. Hukum pidana konvensional yang berfokus pada pelaku individu tidak lagi memadai dalam konteks AI generatif. Oleh karena itu, perlu dikembangkan model pertanggungjawaban multi-aktor yang mencakup pengguna, pengembang, dan penyedia platform. Di Uni Eropa, regulasi AI mulai mengarah pada pembebanan kewajiban kepada seluruh pihak yang terlibat dalam siklus hidup AI, termasuk pengembang dan penyedia system (European Union, 2025). Selain itu, konsep *strict liability* dan *risk-based liability* dapat dipertimbangkan untuk kasus-kasus tertentu yang memiliki risiko tinggi, sehingga tidak selalu bergantung pada pembuktian *mens rea*.

Keempat, reformulasi hukum harus mencakup penguatan kewajiban transparansi dan akuntabilitas AI. Dalam *AI Act*, salah satu kewajiban utama adalah transparansi, termasuk kewajiban untuk mengungkapkan bahwa suatu konten dihasilkan oleh AI serta memastikan bahwa sistem tidak menghasilkan konten ilegal (European Parliament, 2023). Bahkan konten seperti deepfake diwajibkan untuk diberi label agar masyarakat mengetahui bahwa konten tersebut merupakan hasil rekayasa AI. Mengadopsi ketentuan serupa untuk meningkatkan perlindungan terhadap masyarakat dan mencegah penyalahgunaan AI generatif.

Kelima, diperlukan penguatan tanggung jawab penyedia platform dan pengembang AI. Dalam kerangka regulasi modern, penyedia dan pengembang tidak lagi dipandang sebagai pihak pasif, melainkan sebagai aktor yang memiliki kewajiban hukum untuk memastikan keamanan dan keandalan sistem AI. Regulasi ini menekankan pentingnya kewajiban *compliance*, termasuk pengujian sistem, dokumentasi teknis, dan pelaporan risiko (European Union, 2025). Oleh karena itu, perlu menetapkan standar minimum bagi pengembang dan platform, seperti kewajiban penerapan sistem deteksi konten ilegal, audit algoritma, dan mekanisme *notice and takedown*.

Keenam, reformulasi hukum harus memperkuat mekanisme pembuktian digital dan forensik AI. Salah satu problem utama dalam kejahatan berbasis AI adalah kesulitan dalam membuktikan keaslian konten dan atribusi pelaku. Oleh karena itu, diperlukan pengakuan yang lebih luas terhadap alat bukti elektronik, termasuk hasil analisis forensik digital berbasis AI. Selain itu, teknologi seperti watermark digital dan sistem pelacakan konten perlu diintegrasikan dalam kerangka hukum sebagai alat bantu pembuktian. Tanpa pembaruan dalam aspek pembuktian, penegakan hukum terhadap kejahatan AI akan sulit dilakukan secara efektif.

Ketujuh, diperlukan harmonisasi antara KUHP baru dan UU ITE. Saat ini, terdapat potensi tumpang tindih dan konflik normatif antara kedua regulasi tersebut, yang dapat menimbulkan ketidakpastian hukum. Reformulasi hukum harus memastikan bahwa kedua

instrumen tersebut saling melengkapi, bukan saling bertentangan. Selain itu, perlu dipertimbangkan pembentukan regulasi payung (*umbrella regulation*) yang secara khusus mengatur AI dan menjadi rujukan bagi berbagai sektor hukum.

Kedelapan, reformulasi hukum harus mencakup penguatan aspek kelembagaan dan pengawasan. Dalam praktiknya, regulasi AI tidak hanya bergantung pada norma hukum, tetapi juga pada keberadaan lembaga pengawas yang memiliki kewenangan untuk mengawasi implementasi dan menegakkan aturan. Dalam *AI Act*, terdapat mekanisme pengawasan dan penegakan hukum yang terintegrasi untuk memastikan kepatuhan terhadap regulasi (European Union, 20245). Pembentukan lembaga khusus atau memperkuat lembaga yang sudah ada untuk mengawasi penggunaan AI.

Kesembilan, penting untuk mengintegrasikan pendekatan berbasis hak asasi manusia (*human rights-based approach*) dalam regulasi AI. Regulasi AI modern menempatkan perlindungan hak fundamental sebagai prioritas utama, termasuk hak atas privasi, kebebasan berekspresi, dan perlindungan dari diskriminasi. Pendekatan ini memastikan bahwa pengembangan dan penggunaan AI tetap berorientasi pada manusia (*human-centric AI*) (European Commission, 2026). Reformulasi hukum tidak hanya berfokus pada aspek teknis dan pidana, tetapi juga pada perlindungan hak-hak dasar masyarakat.

Terakhir, diperlukan penguatan kerja sama internasional dalam penanggulangan kejahatan berbasis AI. Mengingat sifat AI yang lintas batas, penegakan hukum tidak dapat dilakukan secara nasional semata. Oleh karena itu, Indonesia perlu menjalin kerja sama dengan negara lain dalam hal pertukaran informasi, ekstradisi, dan penanganan kejahatan siber. Harmonisasi dengan standar internasional juga penting agar regulasi nasional tidak tertinggal dari perkembangan global.

4. Kesimpulan

Perkembangan artificial intelligence (AI) generatif telah membawa perubahan fundamental dalam pola kejahatan modern, yang tidak lagi bergantung pada metode konvensional, melainkan memanfaatkan teknologi canggih dengan tingkat kompleksitas tinggi. Berbagai bentuk penyalahgunaan AI generatif, seperti deepfake, impersonasi digital, penyebaran disinformasi, hingga eksploitasi konten non-konsensual, menunjukkan bahwa teknologi ini dapat menjadi instrumen yang memperluas jangkauan dan dampak tindak pidana. Dalam perspektif hukum pidana, fenomena ini menimbulkan tantangan serius, terutama dalam mengkualifikasikan perbuatan, menentukan subjek hukum, serta membuktikan unsur kesalahan.

Pertanggungjawaban pidana menunjukkan bahwa pendekatan konvensional yang berfokus pada pelaku individu tidak lagi memadai. Keterlibatan berbagai aktor dalam ekosistem AI—seperti pengguna, pengembang, dan penyedia platform—menuntut adanya pendekatan baru yang lebih komprehensif dan berbasis pada distribusi tanggung jawab. Selain itu, karakteristik AI yang bersifat otonom dan kompleks juga menimbulkan kesulitan dalam pembuktian *mens rea* serta hubungan kausal antara perbuatan dan akibat, sehingga membuka ruang terjadinya kesenjangan pertanggungjawaban (*responsibility gap*).

Kajian terhadap KUHP baru dan UU ITE menunjukkan adanya berbagai celah hukum yang signifikan. Kedua instrumen hukum tersebut belum secara eksplisit mengatur penyalahgunaan AI generatif, sehingga penegakan hukum masih bergantung pada interpretasi terhadap norma yang bersifat umum. Keterbatasan ini terlihat dalam aspek pengaturan substansi, pertanggungjawaban pidana, pembuktian digital, hingga atribusi pelaku dan yurisdiksi. Selain itu, potensi tumpang tindih antara KUHP baru dan UU ITE juga menimbulkan ketidakpastian hukum dalam praktik. Oleh karena itu, reformulasi hukum menjadi kebutuhan yang mendesak untuk menjawab problem yang ditimbulkan oleh AI generatif. Reformulasi tersebut harus dilakukan secara komprehensif, mencakup pembentukan regulasi khusus AI, penerapan pendekatan berbasis risiko, penyesuaian konsep pertanggungjawaban pidana, serta penguatan mekanisme pembuktian digital.

Di samping itu, harmonisasi antar regulasi, penguatan peran platform dan pengembang, serta integrasi prinsip hak asasi manusia juga menjadi elemen penting dalam pembaruan hukum. Dengan demikian, dapat ditegaskan bahwa tanpa adanya reformulasi hukum yang adaptif dan responsif, sistem hukum pidana Indonesia akan menghadapi kesulitan dalam

mengimbangi perkembangan teknologi AI generatif. Pembaruan hukum tidak hanya diperlukan untuk menutup celah hukum yang ada, tetapi juga untuk memastikan bahwa hukum tetap mampu memberikan kepastian, keadilan, dan perlindungan yang efektif bagi masyarakat di era digital.

Daftar Pustaka

Aprianti, D., & Jamba, P. (2026). Artificial Intelligence and Criminal Liability: Reassessing Mens Rea in the Indonesian and Global Context. *Jurisprudensi: Jurnal Ilmu Syariah, Perundang-Undangan dan Ekonomi Islam*, *18*(1), 106-120. https://doi.org/10.32505/jurisprudensi.v18i1.12804

Arlando Israel Kamasi, A. Timomor, & Meiske M. W. Lasut. (2026). Perlindungan Korban Rekayasa Digital Berbasis Artificial Intelligence Terhadap Data Pribadi Dalam Perspektif Hukum Pidana Indonesia. *Jurnal Sosial Humaniora Dan Pendidikan*, *5*(2), 403–413. https://doi.org/10.55606/inovasi.v5i2.6133

Azzahra, Talitha Dzakiyah., & Lukitasari, Diana. (2025). Perlindungan Korban Tidak Pidana Pemalsuan Identitas Artificial Intelligence pada KUHP 2023. *Jurnal Hukum Pidana dan Penanggulangan Kejahatan*, *14*(2), 165-175. https://doi.org/10.20961/recidive.v14i2.99191

Chairani, M. A., Yitawati, K., & Pradhana, A. P. (2024). Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake. *JURNAL RECHTENS*, *13*(1), 81–96. https://doi.org/10.56013/rechtens.v13i1.2668

Dian Ningtias, A., Nabilah, W., & Ardiansyah, D. (2025). Attributing Legal Responsibility for Deepfake Pornography Generated by Artificial Intelligence: A Juridical Analysis. *Jurnal Independent*, *13*(2), 140–151. https://doi.org/10.30736/ji.v13i2.384

Diel, A., Lalgi, T., Mellis, F. *et al.* (2025). The harm of deepfakes: a scoping review of deepfakes' negative effects on human mind and behavior. *AI & Soc*. https://doi.org/10.1007/s00146-025-02774-0

EUR-Lex. (n.d.). *Rules for trustworthy artificial intelligence in the EU*. https://eur-lex.europa.eu/EN/legal-content/summary/rules-for-trustworthy-artificial-intelligence-in-the-eu.html

European Commission. (n.d.). *Navigating the AI Act*. https://digital-strategy.ec.europa.eu/en/faqs/navigating-ai-act

European Commission. (n.d.). *Regulatory framework for artificial intelligence*. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Parliament. (2023). *EU AI Act: First regulation on artificial intelligence*. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Fajriansyah, Agung., Siregar, Rospita Adelina., & Panggabean, Mompang L. (2025). Reformasi Hukum Pidana di Era Digital: Analisis terhadap KUHP Baru. *Jurnal Hukum Mimbar Justitia (JHMJ)*, *11*(1), 218-230. https://doi.org/10.35194/jhmj.v11i1.5462

Firdaus, Hazmin Sulton., & Puspita, Lona. (2025). Peran Hukum dalam Mengatasi PenyebaranKonten Deepfake untuk Penipuan Identitas Digital. *UIR Law Review*, 9(1), 1-14. https://doi.org/10.25299/uirlrev.2024.vol8(2).22095

Fitriya, R., Furqon, F., Nurfatah, I., Nugraha, B. A., Nasyruddin, A., & Candra, F. A. (2026). Melacak Jejak Pidana AI: Status Subjek Hukum dan Model Pertanggungjawaban di Indonesia. *As-Syar I: Jurnal Bimbingan & Konseling Keluarga*, *8*(1), 48–57. https://doi.org/10.47467/as.v8i1.10277

Ganjar, S. D. (2025). Urgensi Pembaruan Hukum Pidana dalam Menanggulangi Kejahatan Siber: Tinjauan Kritis Terhadap Kesesuaian KUHP Nasional dan Perubahan UU ITE. *Locus*

Journal of Academic Literature Review, *4*(3), 197–208. https://doi.org/10.56128/ljoalr.v4i3.478

Haris, M. T. A. R., & Tantimin, T. (2022). Analisis Pertanggungjawaban Hukum Pidana terhadap Pemanfaatan Artificial Intelligence di Indonesia. *Jurnal Komunikasi Hukum (JKH)*, *8*(1), 307–316. https://doi.org/10.23887/jkh.v8i1.44408

Hutapea, N. M. S., Sitepu, D. K. C., Damanik, C., & Sianipar, S. K. L. (2025). Artificial Intelligence and Criminal Liability: A Preliminary Study within the Indonesian Legal System. *JIHK*, *7*(2), 688-704. https://doi.org/10.46924/jihk.v7i2.330

Lin, L. S. F. (2025). Organisational Challenges in US Law Enforcement's Response to AI-Driven Cybercrime and Deepfake Fraud. *Laws*, *14*(4), 46. https://doi.org/10.3390/laws14040046

Mai, K. T., Bray, S., Davies, T., & Griffin, L. D. (2023). Warning: Humans cannot reliably detect speech deepfakes. PLoS ONE 18(8): e0285333. https://doi.org/10.1371/journal.pone.0285333

Muhammad Afif. (2025). Tindak Pidana Deepfake Pornography di Indonesia: Analisis Yuridis terhadap Kekosongan Norma dalam KUHP dan UU ITE. *MERDEKA: Jurnal Ilmiah Multidisiplin*, *3*(2), 27-35. https://doi.org/10.62017/merdeka.v3i2.6133

Prayoga, D. K., & Edrisy, I. F. (2025). Urgensi Pengaturan Hukum terhadap Deepfake sebagai Alat Kejahatan Siber dalam Perspektif KUHP dan UU ITE. *Journal Evidence of Law*, *4*(3), 1666–1673. https://doi.org/10.59066/jel.v4i3.1865

PwC. (2024). *Artificial intelligence regulation adopted in the EU*. https://www.pwc.com/ua/en/publications/tax-and-legal-alert/2024/artificial-intelligence-regulation-adopted-eu.html

Rahman, R. A., & Habibulah, R. (2019). The Criminal Liability of Artificial Intelligence: Is It Plausible to Hitherto Indonesian Criminal System?. *Legality: Jurnal Ilmiah Hukum*, *27*(2), 147–160. Retrieved from https://ejournal.umm.ac.id/index.php/legality/article/view/10153

Ramadan, M., & Wahyudi, E. (2025). Studi Komparatif: Urgensi Reformulasi Sanksi Pidana Deepfake dalam KUHP dan UU ITE. *JURNAL HUKUM SEHASEN*, *11*(2), 353-362. https://doi.org/10.37676/jhs.v11i2.9463

Ramadhani, M., Hidayat, R., & Hosnah, A. U. (2025). Pertanggungjawaban Pidana atas Tindak Pidana yang Dihasilkan Oleh Sistem AI Otonom (Self-Learning Algorithm): Kajian terhadap Asas Kesalahan dalam Hukum Pidana Indonesia. *Jurnal Review Pendidikan Dan Pengajaran*, *8*(4), 9355–9363. https://doi.org/10.31004/jrpp.v8i4.55259

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

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

Wafi, M. S., Wisnubroto, A., & Prayudi, Y. (2025). Artificial Intelligence-Based Deepfake Crimes: A Conception of Culpability Principle as a Criminal Liability Reform. *Reformasi Hukum*, vol. 29, no. 2, pp. 168–183. doi: 10.46257/jrh.v29i2.1304.

Yodiansyah, A., Farida, A., & Pramono, A. (2026). Dilema Mens Rea pada Algoritma Self-Learning: Siapa yang Bertanggung Jawab Pidana Ketika AI Melakukan Diskriminasi Sistemik?. *Lex Journal: Kajian Hukum Dan Keadilan*, *10*(2), 358-374. https://doi.org/10.25139/lex.v10i2.11870