JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik
E-ISSN: 2747-1993
P-ISSN: 2747-2000
https://dinastirev.org/JIHHP dinasti.info@gmail.com +62 811 7404 455

DOI: https://doi.org/10.38035/jihhp.v6i5
https://creativecommons.org/licenses/by/4.0/
Received: 20 Juni 2026 | **Revised**: 30 Juli 2026 | **Accepted**: 16 Agustus 2026

Limitasi Normatif Pertanggungjawaban Pidana atas Penyalahgunaan Deepfake Berbasis Artificial Intelligence di Indonesia

Gunawan[1]
[1] Universitas Panca Bhakti Pontianak, Pontianak, Indonesia, gunawanfhupb@gmail.com

Corresponding Author: gunawanlay93@gmail.com

Abstract: *This study analyzes the normative limitations of criminal liability for the misuse of deepfake technology based on Artificial Intelligence in Indonesia. The research object is the positive criminal law provisions in the 2024 Electronic Information and Transactions Law (ITE Law), the 2022 Personal Data Protection Law (PDP Law), and the 2023 Criminal Code (KUHP), which have not yet adequately accommodated deepfake misuse. This study aims to analyze the concrete mechanisms of normative limitations in Indonesian positive law and to formulate a more adaptive criminal liability reconstruction model. Using a normative juridical method with statutory, conceptual, and comparative approaches to the EU AI Act 2024, this research finds four concrete limitations: the failure to construct actus reus against synthetically generated content, the inability to prove mens rea (particularly dolus eventualis), the absence of corporate criminal liability regulation against AI platform providers, and norm fragmentation across three statutes. Based on Moeljatno's Dualistic Theory of Criminal Liability and Radbruch's Three Basic Values of Law, Indonesian law remains confined to formal legal certainty without adequately realizing substantive justice or social utility. This research proposes the reconstruction of a specific deepfake offense and the expansion of corporate criminal liability through Articles 45-47 of the 2023 Criminal Code.*

Keyword: *Deepfake, Artificial Intelligence, Pertanggungjawaban Pidana, Limitasi Normatif, Corporate Criminal Liability*

Abstrak: Penelitian ini menganalisis limitasi normatif pertanggungjawaban pidana atas penyalahgunaan teknologi deepfake berbasis *Artificial Intelligence* di Indonesia. Objek penelitian adalah ketentuan hukum pidana positif dalam UU ITE 2024, UU Perlindungan Data Pribadi 2022, dan KUHP 2023 yang belum memadai mengakomodasi penyalahgunaan *deepfake*. Penelitian ini bertujuan menganalisis mekanisme konkret limitasi normatif hukum positif Indonesia dan merumuskan model rekonstruksi pertanggungjawaban pidana yang lebih adaptif. Menggunakan metode yuridis normatif dengan pendekatan *statutory*, *conceptual*, dan *comparative* terhadap EU AI Act 2024, penelitian ini menemukan empat limitasi konkret: kegagalan mengkonstruksi *actus reus* terhadap konten sintetis, ketidakmampuan membuktikan mens rea khususnya *dolus eventualis*, kekosongan pengaturan *corporate criminal liability*

terhadap penyedia platform AI, dan fragmentasi norma yang tersebar di tiga undang-undang. Berdasarkan Teori Pertanggungjawaban Pidana Dualistis Moeljatno dan Teori Tiga Nilai Dasar Hukum Radbruch, hukum Indonesia terjebak pada kepastian hukum formal yang tidak diimbangi keadilan substantif maupun kemanfaatan perlindungan masyarakat. Penelitian ini mengusulkan rekonstruksi delik khusus *deepfake* dan perluasan *corporate criminal liability* melalui Pasal 45-47 KUHP 2023.

Kata Kunci: *Deepfake, Artificial Intelligence*, Pertanggungjawaban Pidana, Limitasi Normatif, *Corporate Criminal Liability*

PENDAHULUAN

Deepfake didefinisikan sebagai konten audiovisual yang dimanipulasi menggunakan teknologi *Artificial Intelligence* generatif, khususnya algoritma *Generative Adversarial Networks* (GAN), sehingga menghasilkan representasi palsu yang sangat mirip dengan identitas asli seseorang (Romero Moreno, 2024). Teknologi ini semakin masif disalahgunakan untuk kejahatan siber, terutama pornografi non-konsensual, penipuan identitas, dan disinformasi politik.

Di Indonesia, kasus penyalahgunaan *deepfake* meningkat tajam. Data PT Indonesia Digital Identity (VIDA) mencatat lonjakan penipuan berbasis *deepfake* sebesar 1.550% antara tahun 2022-2023 (VIDA, 2024). Salah satu kasus konkret yang dapat diverifikasi adalah penipuan *deepfake* yang diungkap Polda Jawa Timur pada April 2025 dengan kerugian mencapai Rp87,6 juta (Kominfo Jatim, 2025).

Dari perspektif *das sollen*, sistem hukum pidana Indonesia seharusnya mampu menjangkau perbuatan pembuatan, distribusi, dan pemanfaatan konten sintetis berbasis AI yang merugikan orang lain. Dari perspektif *das sein*, kondisi teknologi *deepfake* justru melampaui kemampuan norma eksisting: *deepfake* bukan sekadar manipulasi dokumen digital biasa, melainkan *synthetic content generation* yang menghasilkan konten baru dari data biometrik korban. Ketidaksesuaian antara *das sein* dan *das sollen* inilah yang melahirkan kekosongan fungsional yang menjadi objek analisis penelitian ini (Rahardjo, 2009).

Mekanisme terjadinya celah tersebut dapat ditelusuri pada tiga titik. Pertama, Pasal 27 ayat (1) dan Pasal 35 UU ITE 2024 secara tekstual mensyaratkan perbuatan mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya konten. Frasa ini berorientasi pada tindakan distribusi, bukan tindakan pembuatan sintetis, sehingga pelaku yang hanya menciptakan konten *deepfake* tanpa mendistribusikannya secara tekstual belum dapat dijangkau norma ini (Darmawan dkk., 2025). Kata "menciptakan" dalam Pasal 35 UU ITE, apabila dibaca secara sistematik, mensyaratkan adanya rujukan konten asli yang dimanipulasi, bukan generasi konten dari nol sebagaimana karakteristik teknis *deepfake* berbasis GAN (Noerman, 2024). Kedua, konsep "data pribadi" dalam Pasal 68 UU Perlindungan Data Pribadi 2022 tidak secara eksplisit memasukkan data biometrik yang digunakan untuk melatih model AI generatif sebagai objek perlindungan pidana, sehingga terdapat ambiguitas normatif (Athallah dkk., 2025). Ketiga, Pasal 407 UU No. 1 Tahun 2023 tentang KUHP, yang terletak dalam Bab tentang Tindak Pidana Kesusilaan Bagian Pornografi, mensyaratkan akibat konkret yang terukur, sementara kerugian akibat *deepfake* sering bersifat psikologis dan reputasional yang sulit dikuantifikasi secara hukum.

Penelitian ini dilandasi oleh Teori Pertanggungjawaban Pidana Dualistis Moeljatno, yang memisahkan secara tegas antara perbuatan pidana (actus reus) yang bersifat objektif-melawan hukum dengan pertanggungjawaban pidana (mens rea) yang bersifat subjektif dan melekat pada diri pelaku (Moeljatno, 1983). Unsur kesalahan mencakup kesengajaan (dolus directus, dolus indirectus, dan dolus eventualis) serta kealpaan (culpa), termasuk kelalaian berat (culpa

lata) yang memiliki kemiripan konseptual dengan recklessness dalam sistem common law (Kristian, 2025).

Penelitian ini juga menggunakan Teori Tiga Nilai Dasar Hukum Gustav Radbruch, yaitu kepastian hukum (Rechtssicherheit), keadilan (Gerechtigkeit), dan kemanfaatan (Zweckmassigkeit), yang berada dalam hubungan ketegangan yang memerlukan penyelesaian melalui prioritas situasional (Radbruch, 1950). Teori ini digunakan untuk mengevaluasi apakah UU ITE 2024, UU PDP 2022, dan KUHP 2023 telah mewujudkan ketiga nilai tersebut secara simultan bagi korban penyalahgunaan deepfake.

Sebagai pembanding, penelitian ini merujuk pada European Union Artificial Intelligence Act (EU AI Act) 2024, yang mengadopsi pendekatan risk-based regulation. Pasal 50-52 EU AI Act mengatur kewajiban transparansi dan pelabelan (watermarking) bagi konten sintetis, suatu mekanisme preventif-hulu yang berbeda dari pendekatan reaktif-hilir yang dianut Indonesia (European Union, 2024).

Tujuan penelitian ini adalah: pertama, menganalisis mekanisme konkret limitasi normatif Pasal 27 ayat (1), Pasal 35 UU ITE 2024, Pasal 68 UU PDP 2022, dan Pasal 407 KUHP 2023 dalam mengkonstruksi unsur tindak pidana, mens rea, serta pembuktian terhadap penyalahgunaan deepfake berbasis AI; dan kedua, merumuskan model rekonstruksi pertanggungjawaban pidana yang ideal di Indonesia dengan mempertimbangkan doktrin corporate criminal liability dan prinsip-prinsip risk-based regulation.

METODE

Penelitian ini menggunakan metode penelitian hukum yuridis normatif (*normative legal research*), yaitu penelitian yang berfokus pada analisis norma hukum sebagaimana terdapat dalam peraturan perundang-undangan, doktrin, dan asas-asas hukum (Marzuki, 2010). Pendekatan yang digunakan meliputi tiga jenis. Pertama, *statutory approach*, yaitu pengkajian sistematis terhadap UU No. 1 Tahun 2024 tentang ITE, UU No. 27 Tahun 2022 tentang PDP, UU No. 1 Tahun 2023 tentang KUHP, dan UU No. 12 Tahun 2022 tentang TPKS. Kedua, *conceptual approach*, yaitu penggunaan konsep actus reus, mens rea, dolus eventualis, corporate criminal liability, dan risk-based regulation sebagai kerangka analisis. Ketiga, *comparative approach* terhadap EU AI Act 2024.

Pemilihan EU AI Act sebagai pembanding (tertium comparationis) didasarkan pada tiga alasan: pertama, statusnya sebagai regulasi AI supranasional pertama yang telah berlaku secara resmi sejak Agustus 2024; kedua, pendekatan *risk-based regulation*-nya yang paling banyak dikaji secara akademik dan paling adaptif terhadap perkembangan teknologi; dan ketiga, relevansinya bagi negara-negara dengan sistem hukum kontinental-civil law yang serupa dengan Indonesia, termasuk negara-negara Asia Tenggara yang mengacu pada kerangka konseptual serupa.

Teknik analisis yang digunakan adalah *gap analysis* untuk mengidentifikasi kesenjangan antara das sein dan das sollen secara sistematis, dan penafsiran purposif (*purposive interpretation*) untuk menafsirkan ketentuan perundang-undangan berdasarkan tujuan pembentukannya. Bahan hukum primer meliputi peraturan perundang-undangan yang disebutkan di atas beserta EU AI Act 2024. Bahan hukum sekunder meliputi literatur hukum dan jurnal ilmiah yang relevan. Analisis dilakukan secara kualitatif-preskriptif, yaitu menganalisis dan menilai norma hukum untuk kemudian memberikan preskripsi perbaikan.

HASIL DAN PEMBAHASAN

Bagian ini menggunakan struktur silogisme hukum, yaitu premis mayor, premis minor, dan konklusi, dengan teori Moeljatno sebagai premis mayor dan norma hukum positif sebagai premis minor, untuk mengidentifikasi limitasi normatif secara deduktif.

Limitasi Normatif Pasal 27 ayat (1) dan Pasal 35 UU ITE 2024

Pertanggungjawaban pidana mensyaratkan terpenuhinya actus reus yang secara normatif teridentifikasi dalam rumusan delik, dan mens rea yang dapat dibuktikan melekat pada diri pelaku pada saat perbuatan dilakukan (Moeljatno, 1983). Pasal 27 ayat (1) UU ITE 2024 menggunakan frasa "mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik." Frasa ini secara tekstual berorientasi pada tindakan penyebaran konten, bukan penciptaan atau generasi konten. Pelaku *deepfake* yang hanya membuat konten tanpa mendistribusikannya belum dapat dijangkau norma ini.

Pasal 35, yang melarang "memanipulasi, menciptakan, mengubah, menghilangkan, merusak Informasi Elektronik," sekilas tampak relevan karena memuat kata "menciptakan." Namun, kata "menciptakan" dalam Pasal 35 harus dibaca secara sistematik dalam keseluruhan konteks pasal tersebut, yakni menciptakan Informasi Elektronik yang tidak otentik dengan mensyaratkan adanya rujukan keaslian. Dalam *deepfake* berbasis GAN, tidak ada konten asli yang dimanipulasi; konten diciptakan dari nol melalui proses generasi sintetis, sehingga terdapat ketidaksesuaian tekstual antara norma dan karakteristik teknis *deepfake* (Darmawan dkk., 2025; Noerman, 2024).

Untuk membuktikan dolus directus, penuntut umum harus membuktikan bahwa pelaku menghendaki secara langsung distribusi konten yang merugikan korban tertentu. Dalam kasus pelaku yang menggunakan aplikasi *deepfake open-source* tanpa komunikasi dengan korban sebelumnya, membuktikan kehendak langsung menjadi sangat sulit. Dolus eventualis lebih mungkin terpenuhi, namun doktrin Indonesia belum memiliki yurisprudensi yang mengembangkan standar pembuktian dolus eventualis untuk kasus-kasus kejahatan berbasis AI (Kristian, 2025).

Berdasarkan analisis di atas, norma Pasal 27 ayat (1) dan Pasal 35 UU ITE 2024 mengalami kekosongan fungsional pada dua lapis: pertama, ketidaksesuaian tekstual pada unsur actus reus yang tidak menjangkau fase generasi deepfake sekalipun memuat kata "menciptakan"; dan kedua, defisit standar pembuktian mens rea untuk pelaku yang menggunakan tool otomatis. Dari perspektif Radbruch, norma ini memenuhi kepastian formal namun defisit dalam dimensi keadilan substantif dan kemanfaatan (Radbruch, 1950).

Limitasi Normatif Pasal 68 UU PDP 2022 dan Pasal 407 KUHP 2023

Pasal 68 UU PDP 2022 mengatur bahwa setiap orang yang dengan sengaja memalsukan data pribadi dapat dipidana. Data biometrik (wajah, suara) secara definitif termasuk kategori data pribadi menurut Pasal 1 angka 1 UU PDP. Namun terdapat dua masalah struktural. Pertama, orientasi normatif Pasal 68 ditujukan kepada pengendali data dan pemroses data dalam ekosistem bisnis pengolahan data, bukan kepada pelaku kejahatan yang menggunakan data biometrik untuk membuat *deepfake* tanpa seizin subjek data. Kedua, sanksi pidana dalam UU PDP 2022 bersifat residual-administratif, dengan pidana sebagai ultimum remedium (Athallah dkk., 2025).

Pasal 407 KUHP 2023, yang mengatur tindak pidana pornografi sebagai delik materiil, mensyaratkan pembuktian akibat konkret berupa kerugian yang dapat diidentifikasi. Deepfake pornografi menghadirkan tantangan pembuktian akibat konkret karena tiga hal: korban tidak selalu mengetahui adanya deepfake dirinya sehingga laporan polisi sering terlambat; kerugian psikologis tidak dapat dikuantifikasi langsung tanpa keterangan ahli psikologi forensik; dan Pasal 407 tidak mengakomodasi sifat korban semu dalam deepfake, di mana konten secara visual ada tetapi tidak merupakan rekaman kejadian nyata.

Dari perspektif Radbruch, Pasal 68 UU PDP 2022 mengalami defisit pada dimensi kemanfaatan karena sanksi administratif tidak memiliki efek jera yang setara dengan dampak masif kejahatan deepfake, sedangkan Pasal 407 KUHP 2023 mengalami defisit pada dimensi keadilan karena norma yang ada tidak mampu memberikan pemulihan yang setara bagi korban deepfake dibandingkan korban pornografi konvensional (Radbruch, 1950).

Fragmentasi Pertanggungjawaban dan Tantangan Pembuktian Forensik Digital

Fragmentasi pertanggungjawaban (split liability) terjadi karena tidak adanya norma lex specialis yang mengintegrasikan pertanggungjawaban pelaku individu, penyedia platform, dan distributor konten dalam satu kerangka hukum yang koheren. Dari perspektif Moeljatno, situasi ini menciptakan kesulitan dalam konstruksi penyertaan (deelneming) karena setiap aktor dalam rantai dapat berargumen tidak memiliki mens rea terhadap perbuatan aktor lain (Moeljatno, 1983). Dari perspektif Radbruch, situasi ini menciptakan defisit ketiga nilai sekaligus: tidak ada kepastian siapa yang bertanggung jawab, korban tidak dapat mengidentifikasi pihak yang dapat dimintai pertanggungjawaban, dan tidak ada efek jera karena tanggung jawab terdilusi.

Pembuktian forensik digital dalam perkara deepfake menghadapi tiga tantangan struktural. Pertama, rantai pengamanan barang bukti (chain of custody) sulit dipertahankan karena konten deepfake yang disebarkan melalui media sosial mengalami kompresi dan pengkodean ulang yang dapat mengubah metadata asli. Kedua, metode deteksi deepfake yang digunakan oleh lembaga forensik belum distandardisasi di Indonesia, sehingga tidak ada standar yang setara dengan standar Daubert yang mengatur keterterimaan keterangan ahli forensik AI (Ashworth & Hirst, 2022). Ketiga, kelangkaan ahli forensik yang memiliki kompetensi spesifik dalam forensik deepfake berbasis AI generatif membatasi kemampuan sistem peradilan dalam mengevaluasi bukti secara akurat (Casey dkk., 2020; Prakoso, 2024).

Analisis Komparatif dengan EU AI Act 2024

EU AI Act 2024 mengatur deepfake melalui Pasal 50-52 dalam kerangka kategori limited risk. Pasal 50 mewajibkan penyedia sistem AI yang menghasilkan synthetic content untuk menggunakan machine-readable watermarking, dengan sanksi administrative fine hingga EUR 15 juta atau 3 persen dari total turnover global. Pasal 52 mengatur tiga kewajiban transparansi: pengungkapan identitas AI kepada pengguna, label visible disclosure pada konten deepfake, dan pengecualian untuk penggunaan artistik, edukatif, dan satire sepanjang disclosure tetap dilakukan (European Union, 2024).

Pengecualian untuk satire dan parodi ini menjawab kekhawatiran kriminalisasi berlebihan yang tidak diantisipasi oleh norma eksisting Indonesia. Hal-hal yang dapat diadopsi Indonesia secara realistis meliputi kewajiban watermarking dan visible disclosure bagi penyedia platform AI yang beroperasi di Indonesia. Hal-hal yang memerlukan adaptasi signifikan meliputi mekanisme administrative fine yang tidak kompatibel langsung dengan arsitektur sanksi administratif Indonesia.

Tabel 1. Komparasi Regulasi Deepfake Indonesia vs. EU AI Act 2024

Aspek Regulasi	Indonesia (Saat Ini)	EU AI Act 2024 (Pasal 50-52)
Pendekatan Regulasi	Reaktif-hilir	Preventif-hulu
Beban Tanggung Jawab	End-user (pengguna akhir)	Multi-layer (platform + end-user)
Transparansi & Pelabelan	Tidak ada kewajiban	Wajib watermarking & disclosure
Pengecualian Satire/Seni	Tidak diatur	Diatur dengan syarat disclosure
Sanksi Korporasi	Belum diatur tegas	Administrative fine hingga EUR 15 juta

Sumber: Diolah penulis berdasarkan analisis komparatif, 2025

Rekonstruksi Model Pertanggungjawaban Pidana

Rekonstruksi model pertanggungjawaban pidana atas *deepfake* berpijak pada empat prinsip: pertama, prinsip *lex certa*, yaitu rumusan delik harus jelas dan dapat diprediksi penerapannya; kedua, prinsip proporsionalitas, yaitu cakupan delik tidak boleh menjangkau ekspresi kreatif yang sah; ketiga, prinsip multi-layer liability, yaitu pertanggungjawaban harus menjangkau seluruh rantai pelaku; dan keempat, prinsip teknologi-agnostik, yaitu rumusan delik harus cukup luas untuk menjangkau teknologi generatif AI yang akan berkembang di masa depan.

Berdasarkan sintesis Teori Moeljatno, pendekatan EU AI Act, dan prinsip-prinsip rekonstruksi di atas, diusulkan rumusan delik sebagai berikut: setiap orang yang dengan sengaja atau karena kelalaian beratnya membuat, memproses, atau mendistribusikan konten audiovisual sintetis berbasis sistem kecerdasan buatan yang secara realistis merepresentasikan identitas pribadi orang lain tanpa persetujuan yang sah sehingga menimbulkan kerugian yang dapat dibuktikan, dipidana dengan pidana penjara paling lama enam tahun dan/atau denda paling banyak satu miliar rupiah. Apabila perbuatan tersebut dilakukan oleh korporasi, pidana pokok berupa denda paling banyak tiga kali pidana denda yang diatur, dan dapat ditambah pidana tambahan berupa pencabutan izin operasional atau pemblokiran akses layanan di wilayah Indonesia.

Penggunaan frasa "atau karena kelalaian beratnya (culpa lata)" secara alternatif dimaksudkan untuk menjangkau dua gradasi kesalahan: pelaku yang dengan sadar membuat *deepfake* merugikan (dolus directus/eventualis) dan pelaku yang secara lalai berat menyebarkan konten tanpa verifikasi keasliannya. Frasa "secara realistis" menetapkan ambang objektivitas, yaitu hanya *deepfake* yang dapat menyebabkan pengamat yang wajar percaya bahwa konten menggambarkan orang yang dimaksud, sehingga menghindari kriminalisasi berlebihan terhadap konten satire atau parodi. Besaran ancaman pidana enam tahun merujuk pada perbandingan dengan Pasal 27 ayat (1) UU ITE dan prinsip proporsionalitas bahwa *deepfake* berdampak setara dengan kejahatan informasi elektronik yang ada (Kristian, 2025).

Pertanggungjawaban pidana korporasi terhadap penyedia platform AI dapat direkonstruksi melalui dua mekanisme. Pertama, mengoptimalkan Pasal 46 dan Pasal 47 KUHP 2023 dengan menggunakan *identification theory*, yaitu manajemen senior platform yang mengetahui potensi penyalahgunaan sistemik tetapi tidak mengambil tindakan dapat diidentifikasi sebagai directing mind korporasi yang lalai. Kedua, kewajiban *due diligence* dalam delik usulan, yaitu platform AI yang mengoperasikan sistem generatif di Indonesia wajib menerapkan *watermarking* dan sistem deteksi *deepfake*, dan kegagalan memenuhi kewajiban ini dapat dikonstruksi sebagai kelalaian berat korporasi.

Penting dicatat bahwa rekonstruksi *corporate criminal liability* yang diusulkan memiliki keterbatasan aplikabilitas terhadap korporasi AI asing yang tidak berdomisili di Indonesia. Hambatan yurisdiksi ini memerlukan solusi melalui perjanjian bantuan hukum timbal balik atau kerangka kerja sama multilateral, serta mekanisme pemblokiran layanan sebagai sanksi alternatif non-pidana. Dengan demikian, rekonstruksi ini baru efektif penuh untuk pelaku dan korporasi domestik (Sembiring, 2025).

KESIMPULAN

Berdasarkan analisis silogistik yang dibangun dalam penelitian ini, dapat disimpulkan dua hal utama yang menjawab tujuan penelitian. Pertama, mengenai limitasi normatif hukum positif Indonesia, terdapat empat limitasi yang bersifat konkret dan mekanistis. Pada dimensi *actus reus*, Pasal 35 UU ITE 2024 mengalami ketidaksesuaian tekstual karena frasa "menciptakan," apabila dibaca secara sistematik, mensyaratkan adanya konten asli sebagai rujukan manipulasi, bukan generasi konten sintetis dari nol sebagaimana karakteristik *deepfake*. Pada dimensi mens rea, tidak ada yurisprudensi yang mengembangkan standar pembuktian *dolus eventualis* untuk kejahatan berbasis AI, sehingga membuka celah impunitas bagi pelaku yang menggunakan *tool* otomatis. Pada dimensi korporasi, tidak ada norma yang secara tegas mengatur *corporate criminal liability* terhadap penyedia platform AI. Pada dimensi pembuktian, ketiadaan standar keterterimaan forensik *deepfake* menciptakan kekaburan norma yang berpotensi melanggar asas *due process*. Berdasarkan Teori Radbruch, ketiga undang-undang yang dikaji baru memenuhi dimensi kepastian formal, namun defisit pada keadilan substantif dan kemanfaatan perlindungan masyarakat.

Kedua, mengenai model rekonstruksi ideal, penelitian ini mengusulkan transformasi dari pendekatan reaktif-hilir menuju preventif-hulu melalui dua instrumen. Pertama, pembentukan delik khusus *deepfake* yang memenuhi asas *lex certa*, termasuk pengecualian untuk satire dan parodi serta standar kerugian yang dapat dibuktikan. Kedua, perluasan *corporate criminal liability* melalui optimalisasi Pasal 46 dan 47 KUHP 2023 dan kewajiban due diligence platform AI, dengan mengadopsi secara selektif mekanisme *watermarking* dan *disclosure* dari Pasal 50-52 EU AI Act. Perlu ditekankan bahwa rekonstruksi *corporate criminal liability* yang diusulkan memiliki keterbatasan aplikabilitas terhadap korporasi asing dan baru efektif penuh jika didukung oleh kerangka kerja sama hukum internasional yang memadai.

Penelitian ini merekomendasikan agar pembentuk undang-undang segera melakukan amandemen terhadap UU ITE atau menerbitkan peraturan pemerintah turunan yang mewajibkan transparansi dan pelabelan digital bagi penyedia platform AI generatif. Penegak hukum disarankan menyusun pedoman bersama mengenai standardisasi rantai pengamanan barang bukti, metode pengujian deepfake yang dapat diterima, dan kualifikasi minimum ahli forensik. Akademisi hukum disarankan mengembangkan yurisprudensi akademik mengenai standar pembuktian dolus eventualis dalam kejahatan berbasis AI. Dalam jangka panjang, diperlukan pembangunan infrastruktur forensik digital nasional yang tersertifikasi serta penguatan perjanjian bantuan hukum timbal balik dengan negara-negara domisili perusahaan teknologi besar.

REFERENSI

Ashworth, A., & Hirst, M. (2022). Principles of criminal law (9th ed.). Oxford University Press.

Athallah, N. B. P., Candra, A., & Sanusi, H. A. (2025). Urgensi dan kecukupan pengaturan deepfake dalam Undang-Undang Informasi dan Transaksi Elektronik di Indonesia. Judge: Jurnal Hukum, 4(1), 45-62. https://journal.cattleyadf.org/index.php/Judge/article/view/2279

Casey, E., Ferraro, M., & Nguyen, L. (2020). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Academic Press.

Darmawan, M. T., Junaidi, A., & Khaerudin, A. (2025). Penegakan hukum terhadap penyalahgunaan deepfake pornografi anak di era artificial intelligence di Indonesia. Jurnal Penelitian Serambi Hukum, 18(1), 42-54. https://journal.uniba.ac.id/index.php/SH/article/view/1257

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. https://artificialintelligenceact.eu/

Hadjon, P. M. (2019). Pengantar hukum administrasi negara. Gadjah Mada University Press.

Hukumonline. (2025). Deepfake menyebar cepat, hukum bergerak lambat. https://www.hukumonline.com/berita/a/deepfake-menyebar-cepat--hukum-bergerak-lambat-lt68f065103ad53/

Kominfo Jatim. (2025). Polda Jatim ungkap kasus penipuan deepfake AI kepala daerah. https://kominfo.jatimprov.go.id/berita/polda-jatim-ungkap-kasus-penipuan-deepfake-ai-kepala-daerah-pelaku-kantongi-keuntungan-hingga-rp87-juta

Kristian, B. (2025). Assessing criminal liability standards for emerging digital crimes. Sabtida Law Review, 7(1), 112-135. https://journal.sabtida.com/index.php/rlr/article/view/86

Marzuki, P. M. (2010). Penelitian hukum. Kencana Prenada Media.

Moeljatno. (1983). Perbuatan pidana dan pertanggungjawaban dalam hukum pidana. Bina Aksara.

Noerman, C. T. (2024). Kriminalisasi deepfake di Indonesia sebagai bentuk perlindungan hukum. Jurnal Hukum Universitas Semarang, 12(2), 145-168. https://journals.usm.ac.id/index.php/julr/article/view/8995

Prakoso, A. (2024). Pembuktian forensik digital dalam perkara kejahatan siber. Jurnal Hukum dan Pembangunan, 54(2), 289-312.

Prayoga, H., & Tuasikal, H. (2025). Penyebaran konten deepfake sebagai tindak pidana. Abdurrauf Law and Sharia, 2(1), 22-38. https://journal.abdurraufinstitute.org/index.php/arlash/article/view/194

Radbruch, G. (1950). Rechtsphilosophie (3rd ed.). Koehler Verlag.

Rahardjo, S. (2009). Ilmu hukum. Citra Aditya Bakti.

Romero Moreno, F. (2024). Generative AI and deepfakes: A human rights approach. International Review of Law, Computers & Technology. https://doi.org/10.1080/13600869.2024.2324540

Sembiring, J. (2025). Criminal liability for misuse of artificial intelligence (AI) in deepfake crimes. International Journal of Multi Science, 6(1), 78-95.

VIDA. (2024). Deepfake fraud in Indonesia surges 1,550%. VIDA Identity Report. https://vida.id/report.