ASAS WA TANDHIM
Jurnal Hukum, Pendidikan & Sosial Keagamaan
ISSN : 2828-0504 Volume 6 Nomor 1 Tahun 2027, 27 - 38

Generative AI, Deepfake, dan Hak Cipta di Indonesia dalam Tinjauan Yuridis

[1]*Ida Ayu Putu Anggie Sinthiya; [2]Ricco Herdiyan Saputra
[1;2]Institut Bakti Nusantara Pringsewu Indonesia
*Penulis Koresponden, idaayuanggie@gmail.com
disubmisi: 26-04-2026 disetujui: 02-06-2026

Abstrak
Kemajuan pesat *Generative AI* menciptakan kekosongan hukum terkait konten *Deepfake* dan pelanggaran hak cipta. Penelitian ini bertujuan menganalisis kedudukan hukum AI serta distribusi pertanggungjawaban antara pengguna dan pengembang. Menggunakan metode yuridis empiris dengan analisis data kualitatif melalui perangkat lunak NVivo 12, penelitian ini melibatkan informan dari kalangan penegak hukum dan akademisi di Lampung. Hasil penelitian menunjukkan bahwa AI saat ini masih berkedudukan sebagai objek hukum, namun memerlukan penerapan Teori Tanggung Jawab Hibrida Digital untuk memetakan beban kesalahan secara proporsional antara niat pengguna dan kelalaian sistem. Disarankan agar Pemerintah Indonesia segera merumuskan regulasi khusus tata kelola AI yang mewajibkan *digital watermarking* guna menjamin transparansi informasi dan perlindungan martabat manusia tanpa menghambat inovasi teknologi.
Kata Kunci: *Generative AI*, *Deepfake*, Pertanggungjawaban Hukum, Hak Cipta, Tanggung Jawab Hibrida.

Abstract
The rapid advancement of Generative AI has created legal vacuums regarding *Deepfake* content and copyright infringement. This research aims to analyze the legal status of AI and the distribution of liability between users and developers. Utilizing socio-legal methods with qualitative data analysis via NVivo 12, this study involves informants from law enforcement and academia in Lampung. The results indicate that AI currently remains a legal object, yet requires the implementation of Digital Hybrid Liability Theory to map fault proportionally between *User* intent and system negligence. It is suggested that the Indonesian Government immediately formulate specific AI governance regulations mandating digital watermarking to ensure information transparency and protect human dignity without hindering technological innovation.
Keywords: Generative AI, *Deepfake*, Legal Liability, Copyright, Hybrid Liability.

Pendahuluan

Kemajuan pesat *Artificial Intelligence (AI)* dengan kemampuan generatif telah mengubah lanskap teknologi digital dan hukum secara mendasar. Secara operasional, Generative AI merujuk pada sistem

algoritma yang mampu memproduksi konten baru berupa teks, gambar, atau audio secara mandiri berdasarkan pola pembelajaran dari mahadata (*Big Data*) (Ajiraga, 2026; Apriadi et al., 2025; Prayogo et al., 2024; Santoso et al., 2025). Salah satu produk turunan dari teknologi otonom ini yang memicu polemik hukum secara global adalah *Deepfake*. Dalam konteks penelitian ini, *Deepfake* didefinisikan secara operasional sebagai teknik manipulasi kecerdasan buatan untuk merekayasa atau mengganti identitas visual dan auditori seseorang dalam sebuah media digital agar tampak sangat autentik dan sulit dibedakan oleh panca indera manusia (Librianti, 2025).

Penggunaan teknologi ini bersinggungan langsung dengan prinsip pelindungan kekayaan intelektual. Merujuk pada Undang-Undang Nomor 28 Tahun 2014, Hak Cipta secara operasional dipahami sebagai hak eksklusif pencipta yang timbul secara otomatis berdasarkan prinsip deklaratif setelah suatu ciptaan diwujudkan dalam bentuk nyata (Rizkia & Fardiansyah, 2022). Permasalahan hukum muncul ketika model algoritma AI dilatih menggunakan miliaran karya berhak cipta melalui proses ekstraksi data (*Data Scraping*) tanpa izin dari kreator aslinya, yang diidentifikasi sebagai *Copyright Infringement* (Kurniawan & Rojabi, 2026). Lebih jauh, luaran *Deepfake* kerap disalahgunakan secara sistematis untuk kampanye disinformasi dan pencemaran nama baik (Ambardi et al., 2025). Hal ini menciptakan wilayah abu-abu (*grey area*) dalam penegakan hukum di Indonesia, terutama terkait sulitnya pembuktian unsur niat jahat (*Mens Rea*) pada mesin otonom, serta ketidakjelasan distribusi pertanggungjawaban antara pengguna akhir (*User*), pembuat instruksi (*Prompt*), dan korporasi penyedia sistem (*Developer*) (Kartadinata, 2026).

Tinjauan literatur terdahulu menunjukkan bahwa riset akademik mengenai kecerdasan buatan di Indonesia masih sangat didominasi oleh pendekatan ilmu komputer yang berfokus pada efisiensi teknis semata (Rahmawati et al., 2025). Kebanyakan artikel yang ada cenderung hanya mengadopsi teori-teori hukum siber dari negara-negara Barat secara mentah, tanpa melakukan penyesuaian dengan konteks sosiokultural dan kerangka perundang-undangan nasional yang memiliki paradigma berbeda (Rosidi & Laritmas, 2026). Sebagai contoh, banyak literatur dan pihak pengembang menggunakan doktrin *Fair Use* (Penggunaan Wajar) dari yurisdiksi Amerika Serikat untuk membenarkan praktik *data scraping* dalam melatih AI, padahal Pasal 44 Undang-Undang Hak Cipta Indonesia memiliki batasan pengecualian yang jauh lebih ketat dan tidak mengakomodasi eksploitasi data latih secara komersial dan masif oleh mesin. Terdapat jurang pemisah antara kemajuan teknis algoritma yang bersifat *Black Box* dengan teori perlindungan hukum klasik. Oleh karena itu, penelitian ini berusaha mengontekstualisasikan doktrin tanggung jawab mutlak (*Strict Liability*) ke dalam realitas era digital agar relevan dengan tata hukum nasional.

Berangkat dari kompleksitas tersebut, tujuan utama penelitian ini adalah untuk menganalisis secara yuridis kedudukan hukum Generative AI serta memetakan mekanisme distribusi pertanggungjawaban hukum yang paling proporsional antara pengguna dan pengembang terkait penyalahgunaan konten *Deepfake* dan pelanggaran hak cipta. Secara spesifik, penelitian ini dirancang untuk mengidentifikasi celah regulasi *(loopholes*) dalam Undang-Undang ITE dan Undang-Undang Hak Cipta, guna merumuskan rekomendasi rekonstruksi regulasi di masa depan (*Ius Constituendum*).

Manfaat akademis dan praktis dari penelitian ini adalah terwujudnya instrumen hukum preventif yang dapat dijadikan pedoman litigasi bagi penegak hukum, seperti kepolisian, kejaksaan, dan hakim, dalam menangani sengketa siber berbasis otomasi. Di samping itu, kepastian hukum yang ditawarkan dari analisis ini diharapkan mampu melindungi eksistensi kreator lokal dan pelaku UMKM dari ancaman pelanggaran kekayaan intelektual (Wiranto, 2023), sekaligus memberikan jaminan keamanan berinovasi bagi para pengembang teknologi di Indonesia tanpa terbentur multitafsir regulasi.

Metode

Penelitian ini menggunakan rancangan penelitian hukum yuridis empiris (*socio-legal research*) yang mengombinasikan pendekatan perundang-undangan (*statute approach*) dengan studi kasus lapangan guna meninjau efektivitas regulasi terhadap fenomena disrupsi digital. Populasi sasaran dalam penelitian ini mencakup seluruh pemangku kepentingan di ranah hukum dan teknologi informasi di Provinsi Lampung, dengan penentuan informan dilakukan melalui teknik *purposive sampling* yang secara spesifik melibatkan tiga akademisi hukum telematika, dua penyidik unit *Cybercrime* Kepolisian Daerah Lampung, serta tiga praktisi pengembang perangkat lunak kecerdasan buatan guna mendapatkan perspektif multidisipliner. Teknik pengumpulan data diimplementasikan melalui metode triangulasi yang mencakup penelusuran dokumen hukum dan wawancara mendalam (*in-depth interview*), di mana instrumen pengumpulan data dikembangkan berupa panduan wawancara semi-terstruktur yang telah divalidasi kelayakannya melalui uji pakar (*expert judgment*) untuk memastikan pertanyaan mampu menggali aspek pertanggungjawaban algoritma dan kelemahan sistem secara presisi (Hidayanto, 2024).

Dalam proses pelaksanaannya, instrumen atau alat bantu primer yang digunakan adalah perangkat lunak analisis data kualitatif *NVivo versi 12 Plus* yang memiliki kecanggihan fitur *auto-coding* dan *node mapping* untuk memetakan transkrip wawancara ke dalam simpul-simpul tematik hukum secara terkomputerisasi, ditunjang oleh akses basis data *Hukumonline Pro* sebagai alat sekunder untuk melacak sejarah putusan

pengadilan. Adapun bahan primer yang digunakan memiliki komposisi berupa regulasi hukum positif yang terdiri dari Undang-Undang Nomor 11 Tahun 2008 tentang ITE beserta perubahannya, Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, dan Undang-Undang Pelindungan Data Pribadi (UU PDP), yang kemudian diintegrasikan dengan bahan sekunder berupa kompilasi 20 literatur jurnal ilmiah bereputasi terbitan lima tahun terakhir terkait *Generative AI*. Seluruh komposisi data yang telah direduksi tersebut kemudian dianalisis menggunakan metode preskriptif-kualitatif melalui tahapan penyajian data sistematis dan penarikan kesimpulan berbasis silogisme hukum, guna memformulasikan mekanisme pertanggung-jawaban perdata dan pidana yang paling ideal terhadap penyalahgunaan konten *Deepfake*.

Tabel 1
Spesifikasi dan Komposisi Alat serta Bahan Penelitian

Kategori	Nama Komponen	Spesifikasi / Komposisi	Fungsi / Tujuan Penggunaan
Alat Primer	Software NVivo 12 Plus	Fitur Node Mapping, Auto-coding, & Word Frequency Query.	Mengekstraksi dan mengkategorikan transkrip wawancara dari informan agar analisis data tidak bias.
Alat Sekunder	Basis Data Hukumonline Pro	Search engine bertenaga AI dengan filter yurisprudensi dan reglement.	Melacak preseden atau putusan pengadilan terdahulu terkait pelanggaran hak cipta digital dan ITE.
Bahan Primer	Regulasi Positif (Statuta)	UU ITE (revisi terbaru), UU Hak Cipta (UU 28/2014), dan UU PDP.	Menjadi pisau analisis utama (dasar dogmatis) dalam menilai kekosongan hukum (rechtvacuüm).
Bahan Sekunder	Literatur Jurnal Ilmiah	20 Artikel Sinta/Scopus (2019-2024) topik *Deepfake* & Hukum Siber.	Membangun kerangka teoretis dan membandingkan novelty (kebaruan) penelitian dengan riset terdahulu.

Tabel di atas menjabarkan secara terstruktur mengenai instrumen teknis dan bahan hukum yang digunakan selama proses penelitian berlangsung. Pada bagian Alat Primer, penggunaan *NVivo 12 Plus* mencerminkan kecanggihan metodologis penelitian ini; perangkat lunak ini tidak hanya menyimpan data, tetapi secara otomatis mampu membaca pola kata (*Word Frequency*) dari hasil wawancara para penyidik *Cybercrime* dan praktisi AI, sehingga objektivitas analisis kualitatif tetap terjaga. Sementara itu, Alat Sekunder berupa *Hukumonline Pro* digunakan untuk mempercepat pencarian data sekunder berkat fitur kecerdasan

buatan yang tertanam di dalamnya. Pada bagian bahan, Bahan Primer komposisinya mutlak diisi oleh tiga undang-undang pilar utama yang mengatur ruang siber di Indonesia. Penggunaan regulasi ini wajib dilakukan karena permasalahan *Generative AI* sangat bersinggungan langsung dengan hak cipta (UU HC), penyebaran berita bohong/pencemaran (UU ITE), dan manipulasi biometrik wajah (UU PDP). Terakhir, Bahan Sekunder membatasi komposisi literatur maksimal berumur lima tahun ke belakang untuk memastikan bahwa referensi yang dikaji relevan dengan perkembangan teknologi AI yang sangat eksponensial.

Hasil dan Pembahasan

Kedudukan Yuridis *Generative AI* dalam Perspektif Subjek dan Objek Hukum

Sebagai landasan empiris dalam membedah isu disrupsi teknologi ini, analisis data kualitatif dilakukan menggunakan fitur *Node Mapping* dan *Word Frequency Query* pada perangkat lunak NVivo 12 Plus terhadap transkrip wawancara informan, yang terdiri dari penyidik *cybercrime*, akademisi hukum, dan praktisi kecerdasan buatan. Hasil ekstraksi data (*auto-coding*) mengerucut pada tiga simpul tematik utama: "Kekosongan Status Hukum AI", "Otomasi Tanpa Niat Jahat (*Mens Rea*)", dan "Ambiguitas Beban Kesalahan". Rekaman data NVivo ini secara empiris mengonfirmasi bahwa di tingkat penegakan hukum praktis, aparat menghadapi kebuntuan litigasi karena instrumen hukum saat ini belum mampu menjangkau entitas non-biologis yang beroperasi secara otonom.

Temuan lapangan tersebut sejalan dengan hasil analisis dogmatis terhadap kerangka hukum positif di Indonesia. Kedudukan *Artificial Intelligence (AI)* generatif saat ini masih diposisikan secara mutlak sebagai objek hukum (res), bukan sebagai subjek hukum mandiri (*Electronic Personhood*). Dalam konstruksi hukum perdata maupun regulasi telematika seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), sistem elektronik secara kaku diinterpretasikan sebagai alat bantu atau instrumen komputasi statis yang tunduk pada kendali penuh manusia (Saraya et al., 2025). Kemampuan otonom *Generative AI* dalam merumuskan teks analitis atau menciptakan citra visual *Deepfake* yang sangat presisi belum mendapatkan pengakuan atribusi legalitas dari pengadilan di Indonesia (Rudi Nopiansyah & MH, 2025).

Namun, telaah literatur memperlihatkan adanya disparitas yang tajam antara realitas arsitektur teknis kecerdasan buatan dengan batasan doktrinal hukum konvensional. *Generative AI* tidak lagi bekerja secara deterministik layaknya perangkat lunak tradisional, melainkan bersifat stokastik dan probabilistik melalui mekanisme pembelajaran mesin

Machine Learning yang menyerap triliunan mahadata *Big Data* (Wibisono & Napitupulu, 2026). Kondisi ini melahirkan kategori baru secara teoretis, yakni "objek hukum berdaya nalar terbatas", di mana algoritma mampu mengambil keputusan yang probabilitas luarannya tidak selalu dapat diprediksi secara eksak oleh penciptanya (Apriadi et al., 2025). Dalam ranah pelindungan kekayaan intelektual, karakteristik ini sering kali menggugurkan syarat orisinalitas, sehingga karya turunan yang diproduksi murni oleh mesin kerap dianulir hak ciptanya dan jatuh ke ranah domain publik akibat absennya karsa manusiawi *human authorship* (Rizkia & Fardiansyah, 2022).

Konsekuensi logis dari status hukum AI yang merupakan perpanjangan tangan otonom ini berimplikasi langsung pada konstruksi teori pertanggungjawabannya. Mengingat entitas algoritma tidak memiliki kecakapan subjek hukum untuk memikul beban pidana maupun perdata (ketiadaan *mens rea* dan ketiadaan aset untuk ganti rugi), maka penelitian ini menitikberatkan pada dua doktrin utama: Teori Tanggung Jawab Pengganti (*Vicarious Liability*) dan Tanggung Jawab Mutlak (*Strict Liability*). Berdasarkan teori tersebut, segala bentuk kerugian hukum yang timbul dari operasi mesin baik itu penyebaran konten manipulatif maupun pelanggaran hak cipta atas data latih harus dibebankan secara proporsional kepada subjek biologis yang memberi instruksi awal (Pengguna/*User*) atau korporasi yang merancang infrastrukturnya (Pengembang/*Developer*) (KHAIR, 2025). Untuk memperjelas pergeseran fungsi algoritma dan implikasi yuridisnya, perbandingan karakteristik hukum sistem elektronik disajikan pada Tabel 2 berikut.

Tabel 2
Perbandingan Karakteristik Hukum Sistem Elektronik

Dimensi Hukum	Sistem Elektronik Konvensional	*Generative AI*	Implikasi Yuridis
Sifat Operasional	Deterministik (Sesuai input)	Stokastik (Probabilistik/Kreatif)	Sulit memprediksi luaran akhir.
Peran Manusia	Kendali penuh secara langsung	Pemberi instruksi awal (*Prompt*)	Pergeseran dari pelaksana menjadi supervisor.
Status Karya	Reproduksi data	Kreasi turunan (*Derivative Work*)	Ketidakpastian kepemilikan hak cipta.
Klasifikasi Hukum	Objek hukum murni	Objek hukum otonom	Urgensi perluasan definisi subjek hukum.

Penjelasan Tabel 2 di atas mengonfirmasi bahwa meskipun secara formal AI masih berstatus objek, karakteristik operasionalnya yang

bersifat stokastik menuntut adanya penafsiran hukum yang lebih progresif. Jika dalam sistem konvensional kesalahan luaran sepenuhnya dapat ditelusuri ke kesalahan input, pada Generative AI terdapat celah di mana algoritma melakukan "halusinasi" atau menghasilkan konten yang tidak pernah diperintahkan secara spesifik. Ketidakmampuan hukum saat ini untuk mengakomodasi sifat otonom ini menciptakan ketidakpastian bagi para inovator di Indonesia yang ingin memanfaatkan AI untuk efisiensi birokrasi maupun industri kreatif. Oleh karena itu, penelitian ini menyarankan adanya klasifikasi "Subjek Hukum Elektronik Terbatas" sebagai jembatan transisi sebelum Indonesia benar-benar siap memberikan status subjek hukum penuh kepada kecerdasan buatan di masa depan.

Distribusi Pertanggungjawaban Hukum atas Konten *Deepfake* dan Pelanggaran Hak Cipta

Pembahasan mengenai pertanggungjawaban hukum dalam kasus penyalahgunaan konten *Deepfake* mengungkapkan adanya kompleksitas dalam pembagian beban tanggung jawab antara pengguna (*User*) dan penyedia platform (*Provider*). Temuan penelitian menunjukkan bahwa dalam kasus pencemaran nama baik, beban utama pertanggungjawaban pidana sesuai Pasal 27 ayat (3) UU ITE tetap berada pada pihak yang mendistribusikan atau mentransmisikan konten tersebut dengan niat jahat. Namun, sering kali terjadi kebuntuan hukum ketika pengguna berargumen bahwa mereka hanya menggunakan alat yang disediakan secara legal tanpa mengetahui bahwa hasilnya akan melanggar hak orang lain. Di sisi lain, perusahaan pengembang teknologi sering kali berlindung di balik doktrin *Safe Harbor* atau pelabuhan aman, dengan menyatakan bahwa mereka hanya menyediakan infrastruktur teknis dan tidak bertanggung jawab atas perilaku pengguna. Kondisi ini menciptakan celah akuntabilitas yang sangat lebar, terutama ketika konten manipulatif tersebut diproduksi secara masif dan otomatis oleh *bot*.

Dalam perspektif hak cipta, temuan ini sejalan dengan teori *Vicarious Liability* atau tanggung jawab pengganti, di mana pihak yang memiliki kemampuan untuk mengontrol tindakan orang lain dan mendapatkan keuntungan ekonomi darinya harus ikut bertanggung jawab. Jika sebuah platform Generative AI dilatih menggunakan data berhak cipta tanpa izin dan kemudian menghasilkan karya serupa yang dikomersialkan, maka pengembang tidak dapat sepenuhnya melepaskan diri dari tuntutan hukum. Hasil wawancara dengan praktisi hukum menunjukkan bahwa pembuktian adanya unsur kesalahan (*fault*) menjadi titik sentral dalam menentukan proporsi ganti rugi materiil. Distribusi tanggung jawab ini dapat dirumuskan melalui sebuah logika konseptual sederhana untuk memetakan beban kesalahan sebagai berikut: $L = (U_i + D_c) \times H$.

Dalam persamaan (1) tersebut, L merepresentasikan *Liability* (Tanggung Jawab Hukum), U_i adalah User Intent (Niat Pengguna), D_c adalah *Developer Control* (Kendali Pengembang/Filter Algoritma), dan H adalah *Harm* (Kerugian yang Timbul). Persamaan ini menunjukkan bahwa tanggung jawab hukum tidak bersifat tunggal, melainkan merupakan akumulasi dari niat subjek manusia dan sejauh mana sistem keamanan yang dibangun oleh pengembang mampu memitigasi risiko tersebut. Jika pengembang sengaja membiarkan sistemnya tanpa filter keamanan untuk menarik lebih banyak pengguna, maka beban tanggung jawab pengembang menjadi semakin besar meskipun niat jahat utama berasal dari pengguna.

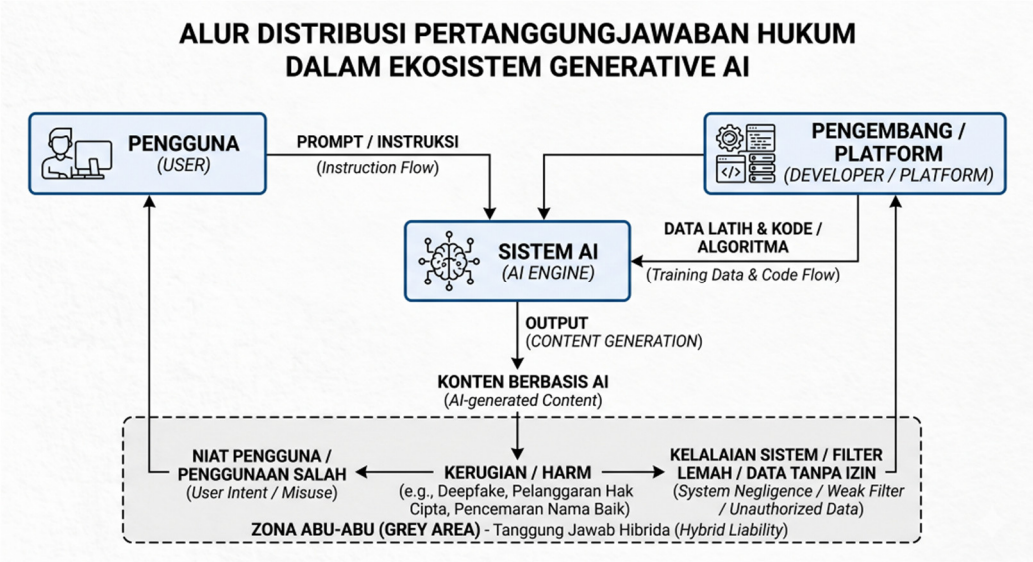
Temuan ini menuntut adanya pembaharuan doktrinal dalam hukum positif. Secara historis, diskursus mengenai pertanggungjawaban hukum bertumpu pada teori tanggung jawab berbasis kesalahan (liability based on fault) peninggalan tradisi Hukum Romawi (Lex Aquilia), yang menetapkan bahwa kompensasi kerugian mutlak mensyaratkan adanya niat jahat (dolus) atau kelalaian (culpa) individu secara langsung dan linier. Memasuki era revolusi industri, doktrin ini berkembang dengan lahirnya teori tanggung jawab mutlak (*Strict Liability*), yang dicetuskan pertama kali oleh Hakim Lord Blackburn melalui preseden klasik hukum umum pada kasus Rylands v. Fletcher (1868), serta doktrin tanggung jawab pengganti (*Vicarious Liability*) yang membebankan kesalahan pada pihak pemegang kendali risiko (Afiftania & Anugerah, 2022). Namun, teori-teori konvensional yang murni berorientasi pada kausalitas subjek biologis tersebut terbukti gagap dan tidak memadai ketika dihadapkan pada entitas kecerdasan buatan yang mampu memproduksi *output* secara probabilistik tanpa kendali langsung manusia.

Oleh karena itu, temuan dalam riset ini mengonstruksikan modifikasi atas sejarah panjang doktrin-doktrin klasik tersebut menjadi sebuah sintesis baru yang penulis deklarasikan sebagai Teori Tanggung Jawab Hibrida Digital. Teori ini menggeser paradigma lama dengan menegaskan bahwa dalam ekosistem AI, kesalahan hukum tidak lagi bersifat individual-linier, melainkan bertransformasi menjadi kolektif-algoritmik. Hal ini sangat aktual dan krusial untuk memecah kebuntuan litigasi pada kasus-kasus manipulasi *Deepfake* di media sosial, yang selama ini hanya menjerat pengguna akhir (kreator kecil) di hilir, sementara perusahaan teknologi raksasa di hulu yang merancang mesin perusak tersebut kerap berlindung di balik kekosongan hukum.

Penafsiran ini sejalan dengan beberapa studi terdahulu yang menekankan urgensi transparansi algoritma sebagai manifestasi pertanggungjawaban publik. Manfaat praktis dari penerapan teori hibrida ini bagi masyarakat adalah terbentuknya mekanisme pelindungan ganda: korban kejahatan siber tidak hanya memiliki legal standing untuk menuntut pelaku penyebar konten, tetapi juga berhak meminta

pertanggungjawaban platform (pengembang) untuk melakukan pemutusan akses *take down* serta menuntut ganti rugi materiil atas kelalaian sistem penyaringan *filter* mereka. Alur pemetaan tanggung jawab hibrida ini—yang mengilustrasikan secara komprehensif bagaimana niat jahat pengguna (*User intent*) dan kelalaian pengawasan sistem (*System negligence*) saling beririsan dalam zona abu-abu pertanggung-jawaban divisualisasikan lebih lanjut dalam Gambar 1 berikut:

Gambar 1
Alur Distribusi Pertanggungjawaban Hukum dalam Ekosistem Generative AI



Sumber: Data diolah oleh Peneliti (2026)

Diagram pada gambar 1, secara sistematis menggambarkan hubungan antara tiga entitas utama (*User*, Sistem AI, dan *Developer/ Platform*) beserta aliran instruksi dan data yang berujung pada potensi kerugian atau *Harm*. Area "Zona Abu-Abu (*Grey Area*)" yang ditandai dengan kotak putus-putus menunjukkan titik di mana tanggung jawab hibrida muncul, yang mengharuskan pembagian akuntabilitas antara niat pengguna (*User intent*) dan kelalaian sistem/filter dari sisi pengembang.

Rekonstruksi Regulasi Masa Depan: Menuju Kedaulatan Digital yang Berkeadilan

Bagian akhir dari pembahasan ini menawarkan proyeksi rekonstruksi regulasi yang harus ditempuh oleh Pemerintah Indonesia melalui konsep *Ius Constituendum* yang lebih adaptif. Hasil penelitian menunjukkan bahwa revisi UU ITE dan UU Hak Cipta saja tidak akan cukup untuk membendung arus disrupsi AI yang sangat cepat; Indonesia membutuhkan sebuah regulasi khusus setingkat Undang-Undang yang secara spesifik mengatur tentang Etika dan Tata Kelola Kecerdasan

Buatan. Regulasi masa depan ini harus mengadopsi prinsip penilaian risiko (*Risk-Based Approach*) sebagaimana yang mulai diterapkan di Uni Eropa melalui *EU AI Act*. Dalam konteks kearifan lokal dan hukum nasional, aturan ini harus menjamin bahwa setiap konten yang dihasilkan oleh mesin wajib disertai dengan label air digital (*Digital Watermarking*) sebagai penanda identitas artifisial. Hal ini penting untuk menjaga transparansi informasi dan mencegah manipulasi opini publik yang dapat merusak tatanan demokrasi dan harmoni sosial di tengah masyarakat.

Tujuan dari rekonstruksi hukum ini adalah untuk menciptakan ekosistem digital yang seimbang antara dorongan inovasi dan perlindungan martabat kemanusiaan. Temuan penelitian menegaskan bahwa tanpa adanya kepastian hukum, para pengembang teknologi lokal akan merasa enggan untuk bereksperimen dengan AI karena takut akan risiko tuntutan hukum yang tidak terukur. Sebaliknya, masyarakat akan merasa tidak aman karena data biometrik dan citra diri mereka dapat dimanipulasi kapan saja tanpa konsekuensi hukum yang jelas bagi pelakunya. Dengan menerapkan standarisasi audit algoritma secara berkala, negara dapat memastikan bahwa setiap teknologi AI yang beroperasi di wilayah kedaulatan digital Indonesia telah memenuhi standar keamanan dan tidak mengandung bias diskriminatif. Langkah ini merupakan bentuk aktualisasi dari fungsi hukum sebagai sarana rekayasa sosial (*Law as a Tool of Social Engineering*) untuk mengarahkan teknologi demi kemaslahatan publik, bukan justru menjadi ancaman bagi peradaban.

Penutup

Kedudukan *Generative AI* dalam sistem perundang-undangan positif di Indonesia saat ini masih diposisikan secara kaku sebagai objek hukum murni, meskipun memiliki karakteristik operasional yang bersifat stokastik dan otonom. Mekanisme pertanggungjawaban hukum atas kerugian imateriil dan materiil yang ditimbulkan oleh konten *Deepfake* dan pelanggaran hak cipta tidak dapat lagi didekati dengan doktrin individual-linier konvensional, melainkan memerlukan penerapan Teori Tanggung Jawab Hibrida Digital yang penulis formulasikan dalam riset ini. Teori ini memetakan bahwa tanggung jawab hukum bersifat akumulatif; pengguna memikul tanggung jawab atas niat jahat penggunaan alat (*direct liability*), sementara pengembang platform harus memikul tanggung jawab pengganti (*vicarious liability*) atas kelalaian dalam filtrasi algoritma dan eksploitasi data latih tanpa izin. Sintesis teoretis ini memberikan kontribusi signifikan terhadap perkembangan khazanah pengetahuan hukum siber Indonesia, sekaligus menjawab kebutuhan mendesak masyarakat akan kepastian hukum substantif di tengah ancaman disrupsi manipulasi informasi yang dapat merusak tatanan harmoni sosial.

Menghadapi dinamika tersebut, penelitian ini memberikan rekomendasi strategis bagi Pemerintah Indonesia untuk segera melakukan rekonstruksi regulasi masa depan (*Ius Constituendum*) melalui penyusunan Undang-Undang khusus mengenai Tata Kelola dan Etika Kecerdasan Buatan yang berkeadilan dan futuristik, tidak cukup hanya mengandalkan revisi parsial atas UU ITE dan UU Hak Cipta yang ada saat ini. Regulasi mutakhir tersebut sebaiknya mengadopsi prinsip penilaian risiko (*Risk-Based Approach*) dan mewajibkan penerapan *Digital Watermarking* pada setiap konten hasil kreasi kecerdasan buatan guna menjamin transparansi serta melindungi martabat manusia dari serangan disinformasi. Bagi praktisi penegak hukum, temuan riset ini dapat diaplikasikan langsung sebagai panduan operasional dalam proses pra-litigasi untuk memetakan beban kesalahan sengketa hibrida siber. Penelitian lanjutan di masa depan sangat disarankan untuk berfokus pada pengembangan metodologi forensik siber teknis yang mumpuni untuk melakukan audit algoritma otonom, guna melengkapi analisis yuridis substantif yang telah dihasilkan dalam tulisan ini.

Daftar Pustaka

Afiftania, L. A., & Anugerah, D. P. (2022). Penerapan Prinsip Vicarious Liability Dalam Pertanggungjawaban Perseroan Terbatas. *Notaire*, *5*(3).

Ajiraga, H. (2026). Peran Dan Tanggungjawab Data Protection Officer Dalam Pelaksanaan Perlindungan Data Pribadi. *Asas Wa Tandhim: Jurnal Hukum, Pendidikan Dan Sosial Keagamaan*, *5*(1), 261–290. Https://Doi.Org/10.47200/Awtjhpsa. V5i1.3209

Ambardi, K., Widhyharto, D. S., Madya, S. H., & Wibawanto, G. R. (2025). *Masyarakat Digital: Teknologi Kekuasaan Dan Kekuasaan Teknologi*. Ugm Press.

Apriadi, E. A., Julianto, R., Dwiatmoko, F., Kom, S., Kom, M., Bisri, M., & Kom, M. (2025). *Kecerdasan Buatan Teori, Implementasi, Dan Aplikasi Di Era Digital*. Eko Aziz Apriadi.

Hidayanto, P. (2024). *Manajemen Digitalisasi Sekolah Di Sekolah Dasar Negeri 2 Patukangan Kabupaten Kendal*. Universitas Pgri Semarang.

Kartadinata, A. (2026). Rekonstruksi Delik Pidana Dalam Kejahatan Deepfake: Tantangan Pembuktian Dan Perlindungan Korban. *Muara Hukum: Jurnal Ilmiah Ilmu Hukum Dan Administrasi Publik*, *2*(1), 36–48.

Khair, M. (2025). *Pertanggungjawaban Hukum Developer Terhadap Pelanggaran Hak Cipta Dalam Penggunaan Generative Artificial Intelligence Berdasarkan Hukum Di Indonesia= Legal Liability Of*

Developers For Copyright Infringement In The Use Of Generative Artificial Intelligence Under Indonesian Law. Universitas Hasanuddin.

Kurniawan, D., & Rojabi, M. A. (2026). *Digital Rights Management Di Balik Era Digitalisasi Masa Kini*. Afdan Rojabi Publisher.

Librianti, E. O. I. (2025). Deepfake Dalam Komunikasi Politik: Tantangan Etika Dan Aspek Hukum Dalam Era Artificial Intelligence. *Siyasah*, *5*(2), 221–238.

Prayogo, P., Korah, R. S. M., Soepeno, M. H., & Kasenda, V. (2024). Analisis Perlindungan Hukum Data Pribadi Nasabah Pada Transaksi Internet Banking Di Sulawesi Utara. *Nuansa Akademik: Jurnal Pembangunan Masyarakat*, *9*(1), 39–54. Https://Doi.Org/10.47200/Jnajpm.V9i4.2089

Rahmawati, A., Amirah, S. N., & Wijaya, N. (2025). Integrasi Kecerdasan Buatan Dalam Pendidikan Tinggi Indonesia: Peluang, Tantangan, Dan Kerangka Implementasi. *Jurnal Teknologi Sistem Informasi*, *6*(1), 114–126.

Rizkia, N. D., & Fardiansyah, H. (2022). *Hak Kekayaan Intelektual Suatu Pengantar*. Penerbit Widina.

Rosidi, A., & Laritmas, S. (2026). *Ilmu Negara Di Era Digital*. Cv. Edu Akademi.

Rudi Nopiansyah, S. H., & Mh, C. P. M. (2025). *Hukum Dan Kecerdasan Buatan: Menyongsong Era Baru Dunia Hukum*. Penerbit Kbm Indonesia.

Santoso, F. S., Takahashi, H., & Reyes, M. C. (2025). Islamic Philanthropy 5.0: Harnessing Big Data And Ai For Zakat, Waqf, And Infaq Optimization. *Journal Islamic Economic Minangkabau*, *3*(4), Article 4. Https://Doi.Org/10.70177/ Jiem.V3i4.2623

Saraya, S., Lubis, A. F., Juansa, A., Layungasri, G. R., & Rianty, E. (2025). *Dinamika Hukum Di Indonesia: Perkembangan & Tantangan*. Pt. Star Digital Publishing, Yogyakarta-Indonesia.

Wibisono, G., & Napitupulu, H. (2026). Mengoptimalkan Big Data Dan Ai Dalam Menentukan Calon Mahasiswa Berkualitas Sebelum Seleksi Perguruan Tinggi. *Riggs: Journal Of Artificial Intelligence And Digital Business*, *4*(4), 673–680.

Wiranto, R. D. (2023). *Perlindungan Hukum Bagi Umkm Terhadap Praktik Monopolo Di Era Digital= Legal Protection For Micro, Small And Medium Enterprises Against Monopoly Practices In The Digital Era*. Universitas Hasanuddin.