Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 8 Nomor 1 Oktober 2026
ISSN (Online): 2714-6917
Halaman 6659-6672

ETIKA PERLINDUNGAN HUKUM TERHADAP DISINFORMASI VISUAL BERBASIS ARTIFICIAL INTELLIGENCE DALAM PERSPEKTIF HUKUM POSITIF DAN HUKUM EKONOMI SYARIAH DI ERA DIGITAL

Lidia Fathaniyah[1*], Euis Nurkholifah[2], Fadli Daud Abdullah[3]
[1] Institut Miftahul Huda Subang, Indonesia
[2] Institut Miftahul Huda Subang, Indonesia
[3] Institut Miftahul Huda Subang, Indonesia

Email: lidiafathaniyah24@gmail.com[1], nurkholifaheuis@gmail.com[2], fadli.daud31@gmail.com[3]

Abstrak
Perkembangan kecerdasan buatan telah meningkatkan penggunaan *deepfake* yang mampu menghasilkan disinformasi visual secara realistis, cepat, dan masif sehingga menimbulkan persoalan perlindungan hukum dan etika di ruang digital. Penelitian ini bertujuan menganalisis perlindungan hukum terhadap disinformasi visual berbasis *Artificial Intelligence* dalam perspektif hukum positif Indonesia dan hukum ekonomi syariah serta merumuskan model tanggung jawab platform digital yang proporsional. Penelitian menggunakan metode kualitatif dengan pendekatan yuridis normatif melalui analisis peraturan perundang-undangan, konsep hukum, literatur, dan regulasi terkait teknologi digital. Hasil penelitian menunjukkan bahwa UU ITE, UU PDP, PP No. 71 Tahun 2019, dan ketentuan perdata telah menyediakan dasar perlindungan, tetapi belum mengatur *deepfake* secara khusus, terintegrasi, dan adaptif. Dalam perspektif hukum ekonomi syariah, *deepfake* yang digunakan untuk menipu atau merugikan bertentangan dengan prinsip kejujuran, amanah, keadilan, serta larangan *tadlis*, *gharar*, dan kebohongan. Penelitian mengusulkan penguatan regulasi melalui pelabelan konten AI, deteksi proaktif, *content provenance*, literasi digital, *AI forensics*, dan model *tiered liability* berbasis kapabilitas platform. Implikasinya adalah perlunya regulasi AI yang mampu memperkuat perlindungan masyarakat tanpa menghambat inovasi teknologi.
Kata Kunci: *Artificial Intelligence*, *Deepfake*, Hukum Ekonomi Syariah, Perlindungan Hukum, Disinformasi Visual.

Abstract
Advancements in artificial intelligence have led to an increase in the use of deepfakes capable of generating realistic visual disinformation rapidly and at scale thereby raising legal and ethical concerns in the digital space. This study aims to analyze legal protections against AI-based visual disinformation from the perspectives of Indonesian positive law and Sharia economic law, and to formulate a proportional liability model for digital platforms. Employing a qualitative method with a normative-juridical approach, the research analyzes relevant legislation, legal concepts, literature, and regulations concerning digital technology. The findings indicate that while the ITE Law, PDP Law, Government Regulation No. 71 of 2019, and civil law provisions provide a basis for protection, they do not yet regulate deepfakes in a specific, integrated, or adaptive manner. From the perspective of Sharia economic law, the use of deepfakes to deceive or cause harm violates principles of honesty, trustworthiness, and justice, as well as prohibitions against tadlis (deception), gharar (uncertainty/ambiguity), and lying. The study proposes strengthening regulations through measures such as AI content labeling, proactive detection, content provenance, digital literacy, AI forensics, and a tiered liability model based on platform capabilities. The

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 8 Nomor 1 Oktober 2026
ISSN (Online): 2714-6917
Halaman 6659-6672

implication is a need for AI regulations that strengthen public protection without stifling technological innovation.
***Keywords**: Artificial Intelligence, Deepfake, Sharia Economic Law, Legal Protection, Visual Disinformation.*

A. Pendahuluan

Perkembangan *Artificial Intelligence* (AI) telah membawa perubahan besar dalam kehidupan digital, terutama dalam produksi dan distribusi informasi. Salah satu perkembangan yang menjadi perhatian adalah *deepfake* dan *synthetic media*, yaitu teknologi yang memanfaatkan *machine learning* untuk menghasilkan atau memanipulasi konten visual dan audio sehingga tampak realistis (Chesney & Citron, 2019). Sebagai latar belakang penelitian, perkembangan tersebut tidak hanya memberikan peluang kreativitas, tetapi juga menghadirkan risiko penyalahgunaan melalui disinformasi visual yang dapat memengaruhi persepsi masyarakat, merusak reputasi, dan menurunkan kepercayaan terhadap informasi digital. Persoalan semakin penting karena penggunaan internet Indonesia mencapai 80,66% atau sekitar 229 juta pengguna pada 2025 (APJII, 2025). Platform seperti TikTok, Facebook, Instagram, dan YouTube menjadi ruang utama penyebaran informasi, sementara rendahnya literasi digital pada sebagian masyarakat, khususnya kelompok pedesaan dan marginal, meningkatkan kerentanan terhadap manipulasi informasi (Kurnia & Astuti, 2021). Konten visual juga sering dianggap sebagai bukti yang sulit dibantah tanpa verifikasi memadai.

Secara empiris, ancaman tersebut semakin terlihat dari meningkatnya penggunaan *deepfake* di Indonesia. Data Kementerian Komunikasi dan Digital menunjukkan bahwa pada periode 2024–2025 terjadi peningkatan sebesar 1.400 persen konten *deepfake* dibandingkan tahun sebelumnya (Yogyakarta, 2026). Sejumlah kasus menunjukkan bahwa teknologi tersebut telah digunakan untuk penipuan dan manipulasi informasi, termasuk video *deepfake* Presiden Joko Widodo yang seolah-olah berbicara dalam bahasa Mandarin pada 2023 serta *deepfake* Presiden Prabowo Subianto pada Januari 2025 yang digunakan dalam modus penawaran bantuan sosial atau dana tunai (DIY, 2025). Kondisi tersebut memperlihatkan bahwa disinformasi visual berbasis AI bukan lagi persoalan teknologi semata, tetapi telah menghasilkan konsekuensi ekonomi, sosial, dan reputasional. Dari perspektif hukum, persoalan tersebut semakin kompleks karena aparat harus menentukan kualifikasi perbuatan, bentuk kesalahan, alat bukti, serta ketentuan yang tepat untuk menjerat pembuat dan penyebar konten manipulatif berbasis AI. Dengan demikian, perkembangan teknologi telah menciptakan bentuk pelanggaran baru yang membutuhkan pendekatan perlindungan hukum yang lebih adaptif.

Landasan teori dalam penelitian ini menggunakan teori perlindungan hukum Philipus M. Hadjon yang membagi perlindungan hukum ke dalam perlindungan preventif dan represif. Perlindungan preventif diarahkan untuk mencegah terjadinya pelanggaran dan kerugian, sedangkan perlindungan represif berkaitan dengan penyelesaian sengketa dan pemulihan hak korban (Setiawan & Babussalam, 2026). Perspektif tersebut dapat dikaitkan dengan konsep negara hukum (*rechtsstaat*) F.J. Stahl yang menempatkan perlindungan hak fundamental warga negara sebagai bagian dari kewajiban negara. Dalam konteks masyarakat digital, pemikiran Satjipto Rahardjo mengenai hukum sebagai instrumen perlindungan masyarakat juga relevan untuk menghadapi dominasi pihak yang memiliki kekuatan teknologi dan ekonomi lebih besar (Annabawi et al., 2025). Sementara itu, perspektif Hukum Ekonomi Syariah

memberikan dasar etis melalui konsep *tadlis* atau penipuan, *gharar* atau ketidakjelasan, dan *al-kadhib* atau kebohongan (Abdullah et al., 2021). Fatwa MUI No. 24 Tahun 2017 menegaskan larangan memproduksi dan menyebarkan konten yang mengandung kebohongan dan fitnah melalui media sosial (Fatwa MUI, 2017). Kerangka teori tersebut digunakan untuk melihat perlindungan korban tidak hanya dari aspek hukum positif, tetapi juga dari prinsip kejujuran, kemaslahatan, dan keadilan dalam syariah.

Gap penelitian terlihat dari keterbatasan hukum positif Indonesia dalam mengatur karakteristik khusus disinformasi visual berbasis AI. UU No. 1 Tahun 2024 tentang Perubahan Kedua UU ITE, UU No. 27 Tahun 2022 tentang PDP, dan PP No. 71 Tahun 2019 telah mengatur berbagai aktivitas digital, tetapi belum memberikan pengaturan khusus mengenai *deepfake*, *synthetic media*, dan *AI-generated content* (Harapan, 2026). Pasal 28 ayat (1) UU ITE mengatur berita bohong dan menyesatkan yang menimbulkan kerugian konsumen, sedangkan Pasal 35 dan Pasal 36 mengatur manipulasi dokumen elektronik dan kerugian pihak lain tanpa secara spesifik mengakomodasi karakteristik *deepfake*. Surat Edaran Menkominfo No. 9 Tahun 2023 tentang Etika Kecerdasan Buatan juga belum memiliki kekuatan mengikat sebagaimana peraturan perundang-undangan (Sudoyo, 2023). Selain itu, UU PDP belum secara eksplisit mengatur *right to one's image* terhadap eksploitasi citra seseorang melalui AI. Kesenjangan tersebut menunjukkan adanya ketidakjelasan norma dalam memberikan perlindungan kepada korban dan menentukan tanggung jawab hukum pelaku.

Gap berikutnya berkaitan dengan tanggung jawab platform media sosial. Regulasi Indonesia belum secara jelas menentukan kewajiban platform dalam melakukan moderasi *deepfake*, penggunaan teknologi deteksi, maupun *labeling* terhadap konten yang dihasilkan AI. Kondisi tersebut berbeda dengan beberapa negara yang telah mengembangkan mekanisme regulasi khusus (Quratuainniza, 2026). Uni Eropa melalui *AI Act* menerapkan pendekatan berbasis risiko, termasuk kewajiban *labeling* terhadap konten *deepfake* dan sanksi administratif hingga €35 juta atau 7% pendapatan global tahunan. Tiongkok melalui *Deep Synthesis Provisions* mewajibkan *watermarking* dan verifikasi identitas pembuat konten, sedangkan Korea Selatan melalui *AI Framework Act* dan Singapura melalui *Online Safety Act* mengembangkan mekanisme pengawasan dan penilaian risiko platform. Novelty penelitian ini terletak pada upaya mengintegrasikan perspektif hukum positif Indonesia dengan Hukum Ekonomi Syariah untuk membangun model perlindungan yang mencakup pencegahan, pertanggungjawaban platform, pemulihan korban, serta prinsip *tadlis*, *gharar*, *al-kadhib*, dan kemaslahatan. Pendekatan tersebut diarahkan untuk menghasilkan konstruksi hukum yang sesuai dengan perkembangan teknologi sekaligus konteks sosio-yuridis masyarakat Indonesia.

Masalah penelitian dalam kajian ini mencakup tiga persoalan utama, yaitu bagaimana pengaturan disinformasi visual berbasis AI dalam hukum positif Indonesia, bagaimana etika perlindungan hukum terhadap disinformasi visual berbasis AI dalam perspektif Hukum Ekonomi Syariah, serta bagaimana konstruksi tanggung jawab hukum platform media sosial dalam memberikan perlindungan yang efektif kepada masyarakat. Tujuan penelitian adalah menganalisis pengaturan disinformasi visual berbasis AI dalam hukum positif Indonesia, mengidentifikasi kekosongan dan keterbatasan norma yang berlaku, serta merumuskan konstruksi tanggung jawab hukum platform media sosial berdasarkan perspektif hukum positif dan Hukum Ekonomi Syariah. Penelitian ini juga diarahkan untuk mempertemukan aspek regulasi dengan prinsip etika sehingga perlindungan terhadap masyarakat tidak hanya berorientasi pada

penindakan setelah kerugian terjadi, tetapi juga pada pencegahan dan pengendalian risiko sejak konten diproduksi dan didistribusikan.

Implikasi penelitian diharapkan memberikan kontribusi pada dua aspek. Secara akademik, penelitian ini dapat memperluas kajian hukum teknologi dan Hukum Ekonomi Syariah, khususnya mengenai perkembangan AI, disinformasi visual, perlindungan hukum, dan tanggung jawab platform digital. Secara praktis, hasil penelitian dapat menjadi bahan pertimbangan bagi pembentuk kebijakan dalam menyusun regulasi yang lebih adaptif terhadap *deepfake* dan *AI-generated content*, termasuk penguatan mekanisme *labeling*, deteksi, moderasi, serta pertanggungjawaban platform. Bagi masyarakat, penelitian ini diharapkan memperkuat perlindungan terhadap kerugian ekonomi, reputasi, dan hak pribadi akibat disinformasi visual. Sementara dari perspektif Hukum Ekonomi Syariah, penelitian ini dapat memperkuat penerapan prinsip kejujuran, keadilan, kemaslahatan, dan larangan *tadlis*, *gharar*, serta *al-kadhib* dalam aktivitas digital sehingga perkembangan teknologi AI tetap berada dalam koridor perlindungan hukum dan etika.

B. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif dengan jenis penelitian kualitatif yang berfokus pada analisis norma, konsep, dan prinsip hukum terkait etika perlindungan terhadap disinformasi visual berbasis *Artificial Intelligence* (AI) (Anggito & Setiawan, 2018). Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) untuk mengkaji peraturan mengenai informasi elektronik, perlindungan data, dan konten digital; pendekatan konseptual (*conceptual approach*) untuk menganalisis konsep perlindungan hukum, disinformasi, AI, serta prinsip Hukum Ekonomi Syariah; pendekatan perbandingan (*comparative approach*) untuk melihat perkembangan pengaturan AI dan *deepfake* dalam beberapa sistem hukum; serta pendekatan analitis (*analytical approach*) untuk menguraikan kesesuaian dan kekosongan norma yang berkaitan dengan objek penelitian. Alat penelitian berupa bahan hukum primer, sekunder, dan tersier, dengan bahan hukum primer mencakup peraturan perundang-undangan terkait informasi elektronik, perlindungan data, dan konten digital, bahan hukum sekunder berupa buku, artikel ilmiah, dan laporan penelitian yang relevan, serta bahan hukum tersier berupa kamus hukum dan dokumen pendukung lainnya (Abdullah et al., 2024). Teknik pengumpulan dat**a** dilakukan melalui studi kepustakaan dengan menginventarisasi, mengklasifikasikan, dan menelaah bahan hukum yang relevan, sedangkan teknik analisis data dilakukan secara kualitatif melalui reduksi bahan hukum, interpretasi, perbandingan, dan penarikan kesimpulan secara sistematis. Metode ini dipilih karena objek penelitian berfokus pada norma hukum dan prinsip etika, bukan pada pengukuran perilaku masyarakat, sehingga mampu mengidentifikasi kesenjangan regulasi serta merumuskan konstruksi perlindungan hukum yang lebih adaptif (Mansari, 2026). Urgensi penelitian terletak pada meningkatnya penggunaan AI untuk menghasilkan disinformasi visual yang berpotensi menimbulkan kerugian ekonomi, reputasi, dan sosial, sedangkan implikasinya diharapkan memberikan kontribusi akademik bagi pengembangan hukum teknologi dan Hukum Ekonomi Syariah serta menjadi bahan pertimbangan dalam membangun regulasi dan mekanisme perlindungan masyarakat yang mengedepankan kepastian hukum, keadilan, pencegahan kerugian, dan kemaslahatan.

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 8 Nomor 1 Oktober 2026
ISSN (Online): 2714-6917
Halaman 6659-6672

C. Hasil dan Pembahasan

1. Kesenjangan Regulasi dan Pergeseran Paradigma Perlindungan Hukum terhadap Disinformasi Visual Berbasis AI di Indonesia

Perkembangan *deepfake* menunjukkan bahwa hukum positif Indonesia masih menghadapi kesenjangan antara perkembangan teknologi dan kemampuan regulasi dalam mengidentifikasi serta menangani bentuk baru disinformasi visual (Akbar et al., 2026). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) belum secara eksplisit mendefinisikan *deepfake* maupun konten *AI-generated* sebagai fenomena hukum tersendiri. Pasal 27 ayat (1) UU ITE dapat diterapkan terhadap *deepfake* bermuatan seksual karena melarang distribusi informasi elektronik yang memiliki muatan melanggar kesusilaan, tetapi jangkauannya terbatas pada aspek kesusilaan. Sementara itu, Pasal 28 ayat (1) berorientasi pada berita bohong dan menyesatkan yang menimbulkan kerugian konsumen dalam transaksi elektronik. Rumusan tersebut menyebabkan disinformasi visual yang berdampak terhadap reputasi, opini publik, atau kepentingan sosial di luar transaksi elektronik tidak sepenuhnya terakomodasi. Hartono et al (2026) juga menunjukkan persoalan ketika konten palsu dihasilkan secara otomatis oleh mesin, karena konstruksi pertanggungjawaban hukum selama ini cenderung berorientasi pada tindakan manusia secara langsung.

Pasal 35 UU ITE memiliki relevansi teknis yang lebih kuat karena mengatur manipulasi Informasi Elektronik dan/atau Dokumen Elektronik agar seolah-olah menjadi data yang autentik. Karakteristik tersebut pada dasarnya beririsan dengan mekanisme *deepfake* yang memanipulasi gambar, video, suara, atau identitas visual sehingga tampak nyata. Bahkan, berdasarkan Pasal 51 UU ITE, pelanggaran tersebut dapat dikenai pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp12.000.000.000,00. Pasal 36 mengenai perbuatan yang mengakibatkan kerugian bagi orang lain juga dapat berfungsi sebagai ketentuan pemberatan. Namun, persoalan muncul karena UU ITE belum menyediakan definisi operasional yang secara tegas menghubungkan teknologi *deepfake* dengan unsur "manipulasi" dalam Pasal 35. Penafsiran yang terlalu ekstensif dalam hukum pidana berpotensi menimbulkan persoalan terhadap prinsip *lex certa*, sehingga diperlukan kepastian mengenai karakteristik perbuatan yang dapat dikategorikan sebagai manipulasi digital. Dengan demikian, permasalahan bukan semata-mata ketiadaan norma, melainkan juga adanya ketidaksesuaian antara norma yang tersedia dengan karakteristik teknologi AI yang bersifat otomatis, masif, dan adaptif.

Celah perlindungan juga terlihat dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang tersebut menempatkan data biometrik sebagai data pribadi yang bersifat spesifik, termasuk karakteristik fisik yang memungkinkan identifikasi seseorang, seperti gambar wajah. Pasal 65 ayat (1) melarang pengumpulan data pribadi milik orang lain tanpa hak, sedangkan Pasal 66 melarang pembuatan data pribadi palsu yang mengakibatkan kerugian bagi orang lain, dengan ancaman pidana berdasarkan Pasal 68 berupa penjara paling lama 6 tahun dan/atau denda paling banyak Rp6.000.000.000,00. Akan tetapi, Aini & Lubis (2024) mengidentifikasi bahwa UU PDP belum secara eksplisit mengakui *right to one's image* atau hak atas citra sebagai bagian dari perlindungan privasi. Persoalan lainnya adalah belum tersedianya peraturan pelaksana yang secara khusus memberikan pedoman teknis mengenai penyalahgunaan data biometrik untuk *deepfake*. Kondisi tersebut memperlihatkan bahwa perlindungan terhadap korban masih terfragmentasi: UU ITE

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 8 Nomor 1 Oktober 2026
ISSN (Online): 2714-6917
Halaman 6659-6672

berorientasi pada manipulasi dan distribusi informasi, sedangkan UU PDP berorientasi pada perlindungan data pribadi.

Persoalan yang paling fundamental kemudian muncul pada posisi platform digital. PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) mewajibkan Penyelenggara Sistem Elektronik (PSE) menyelenggarakan sistem yang andal, aman, dan bertanggung jawab serta memberikan kewenangan kepada pemerintah untuk menjatuhkan denda Rp100 juta hingga Rp500 juta per konten negatif yang dibiarkan beredar oleh platform (Komdigi, 2019). Dalam UU ITE, platform berkedudukan sebagai PSE atau *intermediary* berdasarkan Pasal 15 dan secara konseptual mendekati doktrin *safe harbour*. Mekanisme yang dikenal meliputi *notice and takedown, notice and notice,* serta *notice and disconnection* (Fadhila, 2026). Akan tetapi, model reaktif tersebut menghadapi keterbatasan ketika diterapkan terhadap *deepfake* karena satu konten dapat direplikasi secara otomatis dalam jumlah besar. Wulandari et al (2025) menunjukkan bahwa mekanisme *notice and takedown* yang dirancang untuk lingkungan *user-generated content* tidak sepenuhnya memadai dalam menghadapi konten AI-generatif. Oleh karena itu, perlindungan hukum perlu bergeser dari model *reactive liability* menuju *proactive responsibility* yang tetap proporsional terhadap kemampuan platform.

Tabel 1. *Pemetaan Kesenjangan Regulasi dan Arah Perlindungan Hukum*

Instrumen Hukum	**Ruang Perlindungan**	**Kelemahan terhadap Deepfake**	**Arah Penguatan**
Pasal 27 ayat (1) UU ITE	Konten bermuatan kesusilaan	Terbatas pada aspek kesusilaan	Perlu klasifikasi khusus terhadap *deepfake* berbahaya
Pasal 28 ayat (1) UU ITE	Berita bohong yang merugikan konsumen dalam transaksi elektronik	Tidak mencakup seluruh dampak reputasi, politik, dan sosial	Memperluas konstruksi perlindungan terhadap kerugian nontransaksional
Pasal 35 jo. Pasal 51 UU ITE	Manipulasi informasi agar tampak autentik	Belum terdapat definisi operasional *deepfake*	Penegasan unsur manipulasi AI dan standar pembuktian
Pasal 36 UU ITE	Kerugian terhadap orang lain	Bersifat pelengkap	Ditempatkan sebagai ketentuan pemberatan sesuai akibat
Pasal 65–66 jo. Pasal 68 UU PDP	Perlindungan data biometrik dan data pribadi palsu	Belum mengatur *right to one's image* dan aspek teknis *deepfake*	Penguatan perlindungan hak atas citra dan aturan pelaksana

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 8 Nomor 1 Oktober 2026
ISSN (Online): 2714-6917
Halaman 6659-6672

PP No. 71 Tahun 2019	Kewajiban PSE dan pengelolaan konten negatif	Belum ada kewajiban khusus deteksi AI	Kewajiban *proactive detection* dan *AI labeling*
Pasal 15 UU ITE	Tanggung jawab PSE	Masih dekat dengan pendekatan *safe harbour*	Pergeseran menuju tanggung jawab berbasis risiko dan kapabilitas
Notice and takedown	Penghapusan konten setelah laporan	Bersifat reaktif dan berpotensi terlambat	*Expedited takedown* dan pencegahan penyebaran ulang

Hasil analisis menunjukkan bahwa hukum positif Indonesia sebenarnya telah memiliki sejumlah instrumen yang dapat digunakan untuk menangani *deepfake*, terutama melalui UU ITE dan UU PDP, tetapi belum memiliki konstruksi hukum yang terintegrasi. Persoalan utama terletak pada ketiadaan definisi operasional, standar pembuktian, perlindungan hak atas citra, serta kewajiban teknis platform. Karena itu, perlindungan hukum terhadap disinformasi visual berbasis AI perlu direkonstruksi dari pendekatan yang semata-mata represif menuju sistem perlindungan preventif, represif, dan administratif yang berbasis risiko serta proporsionalitas.

2. Deepfake sebagai Tadlis Teknologis: Rekonstruksi Etika Perlindungan Hukum Berdasarkan Maqasid al-Syariah

Dalam perspektif hukum ekonomi syariah, persoalan *deepfake* tidak hanya berkaitan dengan legalitas suatu konten, tetapi juga dengan etika produksi, distribusi, dan pemanfaatan teknologi. Fiqh muamalah meletakkan kejujuran (*sidq*), kejelasan (*bayyinah*), keadilan (*adl*), amanah, serta larangan *gharar* dan *tadlis* sebagai prinsip fundamental dalam hubungan muamalah. *Deepfake* yang dibuat untuk menciptakan persepsi seolah-olah suatu peristiwa benar-benar terjadi dapat dikonstruksikan sebagai bentuk *tadlis* teknologis karena kepalsuan disembunyikan melalui teknologi sehingga pengguna menerima informasi yang berbeda dari kenyataan. Pada saat yang sama, konten tersebut menciptakan *gharar* karena masyarakat mengalami ketidakjelasan mengenai batas antara fakta dan rekayasa. Apabila disertai kesengajaan untuk menyampaikan informasi palsu, *deepfake* juga mengandung unsur *al-kadhib* atau kebohongan. Dengan demikian, permasalahan *deepfake* dalam HES memiliki dimensi etika yang lebih luas daripada sekadar pelanggaran hukum positif.

Pertanggungjawaban tersebut tidak hanya melekat pada pembuat konten, tetapi dapat dianalisis terhadap pihak yang secara aktif memfasilitasi penyebarannya. QS. Al-Maidah ayat 2 memberikan dasar mengenai larangan *ta'awun 'ala al-itsm wa al-'udwan*, yaitu membantu dalam perbuatan dosa dan permusuhan. Dalam konteks platform digital, algoritma rekomendasi yang secara aktif memperkuat konten berdasarkan *engagement* dapat menjadi objek kajian etis ketika sistem tersebut mengetahui atau secara sistematis memperbesar distribusi konten yang berbahaya. Prinsip *al-ghurm bi al-ghunm* juga relevan, yaitu risiko sebanding dengan keuntungan: pihak yang memperoleh keuntungan dari suatu aktivitas pada prinsipnya memikul konsekuensi risiko yang timbul dari aktivitas tersebut. Oleh sebab itu, ketika platform memperoleh keuntungan ekonomi dari distribusi konten *deepfake*, terdapat dasar etis-syar'i untuk membebankan kewajiban pencegahan dan penanganan yang proporsional. Argumentasi

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 8 Nomor 1 Oktober 2026
ISSN (Online): 2714-6917
Halaman 6659-6672

tersebut memperkuat bahwa tanggung jawab platform tidak seharusnya selalu diposisikan sebagai tanggung jawab pasif.

Analisis *maqasid al-syariah* semakin memperlihatkan bahwa dampak *deepfake* dapat menyentuh beberapa tujuan fundamental syariah. Al-Ghazali (1997) mengidentifikasi *al-kulliyyat al-khams*, dan dalam konteks penelitian ini setidaknya terdapat tiga aspek yang sangat relevan, yaitu *hifzh al-'aql* atau perlindungan akal, *hifzh al-mal* atau perlindungan harta, dan *hifzh al-'ird* atau perlindungan kehormatan. Disinformasi visual mengganggu kemampuan masyarakat membedakan fakta dan rekayasa sehingga mengancam *hifzh al-'aql*. *Deepfake* finansial, seperti pemalsuan identitas pejabat atau tokoh tertentu untuk penipuan investasi, dapat menyebabkan kerugian harta sehingga berkaitan dengan *hifzh al-mal*. Sementara *deepfake* seksual non-konsensual dan pencemaran nama baik dapat merusak martabat seseorang sehingga berkaitan dengan *hifzh al-'ird*. Oleh karena itu, kewajiban *labeling*, deteksi proaktif, *expedited takedown*, dan mekanisme pelaporan bukan hanya instrumen teknis, tetapi dapat ditempatkan sebagai sarana mencapai *maslahah* dan mencegah *mafsadah*.

Fatwa MUI No. 24 Tahun 2017 tentang Hukum dan Pedoman Bermuamalah Melalui Media Sosial memperkuat dimensi etis tersebut. Fatwa tersebut menetapkan kewajiban *tabayyun* sebelum menyebarkan informasi dengan merujuk QS. Al-Hujurat ayat 6, mengharamkan produksi, penyebaran, dan membuat dapat diaksesnya konten yang tidak benar, serta menyatakan haram aktivitas buzzer yang menyebarkan hoaks dan fitnah untuk memperoleh keuntungan ekonomi (Fatwa, 2017)Dalam konteks *deepfake*, prinsip tersebut menunjukkan adanya perbedaan antara penggunaan teknologi untuk kepentingan artistik, edukatif, atau hiburan yang transparan dan penggunaan teknologi untuk menipu atau merugikan pihak lain. Kaidah *ma la yatimmu al-wajib illa bihi fahuwa wajib* juga dapat menjadi dasar argumentasi bahwa apabila pencegahan kerusakan informasi membutuhkan mekanisme teknis tertentu, maka penggunaan mekanisme tersebut dapat menjadi bagian dari kewajiban. Dengan demikian, teknologi *deepfake* tidak otomatis haram berdasarkan teknologinya, tetapi status etis-syar'inya ditentukan antara lain oleh tujuan, cara penggunaan, transparansi, dan akibat yang ditimbulkannya.

Tabel 2. *Analisis Etika Deepfake Berdasarkan Hukum Ekonomi Syariah*

Prinsip HES	**Manifestasi Deepfake**	**Risiko**	**Prinsip Perlindungan**
Sidq	Konten palsu disajikan seolah-olah benar	Hilangnya kepercayaan	Kejujuran dan pelabelan AI
Tadlis	Kepalsuan disembunyikan melalui manipulasi visual	Penipuan dan kesesatan informasi	Disclosure dan transparansi
Gharar	Pengguna tidak mengetahui apakah konten autentik	Ketidakpastian dan sengketa	*Content provenance* dan verifikasi
Al-kadhib	Informasi palsu sengaja disebarkan	Kerusakan sosial dan reputasi	*Tabayyun* dan moderasi
Ta'awun 'ala al-itsm	Platform secara aktif memperkuat konten berbahaya	Percepatan penyebaran mafsadah	Tanggung jawab algoritmik

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 8 Nomor 1 Oktober 2026
ISSN (Online): 2714-6917
Halaman 6659-6672

Al-ghurm bi al-ghunm	Platform memperoleh keuntungan dari *engagement*	Risiko dibebankan sepenuhnya kepada korban	Tanggung jawab proporsional platform
Hifzh al-'aql	Manipulasi persepsi publik	Rusaknya kemampuan membedakan fakta	Labeling dan literasi digital
Hifzh al-mal	Penipuan investasi/keuangan berbasis *deepfake*	Kerugian finansial	Deteksi proaktif dan *fast-track takedown*
Hifzh al-'ird	*Deepfake* seksual dan pencemaran nama baik	Kerusakan kehormatan	Pelaporan mudah dan penghapusan cepat

Dalam perspektif HES, *deepfake* yang mengandung penipuan atau kerugian dapat dipahami sebagai bentuk *tadlis* dan *al-kadhib*, sementara kondisi ketidakpastian yang diciptakannya mengandung dimensi *gharar*. Melalui *maqasid al-syariah*, perlindungan terhadap akal, harta, dan kehormatan memberikan dasar normatif bagi penguatan tanggung jawab platform. Dengan demikian, perlindungan terhadap *deepfake* tidak hanya berorientasi pada penghukuman pelaku, tetapi juga pada penciptaan ekosistem digital yang menjaga *maslahah*, amanah, transparansi, dan keadilan.

3. Rekonstruksi Norma Berbasis Tiered Liability: Membangun Tanggung Jawab Platform yang Preventif, Proporsional, dan Beretika Syariah

Kesenjangan regulasi dan persoalan etika tersebut menunjukkan kebutuhan untuk melakukan rekonstruksi norma yang lebih operasional. Langkah pertama adalah menetapkan definisi yang komprehensif mengenai disinformasi visual berbasis AI, *deepfake*, dan platform bertanggung jawab. Disinformasi visual berbasis AI dapat dirumuskan sebagai konten visual berupa gambar atau video yang dibuat atau dimodifikasi secara substansial menggunakan teknologi AI sehingga merepresentasikan seseorang, peristiwa, atau keadaan yang tidak nyata atau terdistorsi secara menyesatkan. *Deepfake* merupakan bentuk khusus disinformasi visual berbasis AI yang secara spesifik mengganti citra wajah, suara, atau identitas visual seseorang menggunakan teknik *machine learning*. Sementara itu, platform bertanggung jawab dapat ditempatkan sebagai PSE yang menyediakan fasilitas distribusi, berbagi, atau publikasi konten dan memiliki kemampuan teknis untuk mendeteksi serta mengelola konten tersebut. Definisi ini penting agar penegakan hukum tidak bergantung pada penafsiran analogis semata.

Berdasarkan perbandingan regulasi internasional yang telah dikemukakan, terdapat tiga pendekatan yang dapat menjadi referensi. Uni Eropa melalui EU AI Act (Regulation EU 2024/1689) menggunakan pendekatan berbasis risiko dan melalui Pasal 50 menetapkan kewajiban transparansi terhadap konten tertentu yang dihasilkan atau dimanipulasi AI, termasuk kewajiban *disclosure* dan pelabelan yang terlihat serta persisten. Sanksi administratif untuk pelanggaran tertentu dapat mencapai €35 juta atau 7% pendapatan global tahunan perusahaan (Febriani et al., 2022). Tiongkok melalui *Administrative Provisions on Deep Synthesis of Internet Information Service* yang berlaku sejak 10 Januari 2023 mewajibkan *watermarking* otomatis, *real-name authentication*, dan registrasi manusia virtual pada platform (Congress, 2023). Sementara itu, model Indonesia berdasarkan UU ITE dan PP No. 71 Tahun 2019 masih

dominan reaktif karena belum mengatur *proactive detection*, kewajiban *AI content labeling*, dan *transparency reporting*. Perbedaan tersebut menunjukkan bahwa Indonesia dapat mengambil prinsip-prinsip yang relevan dari kedua yurisdiksi tanpa harus menyalin keseluruhan model regulasinya.

Atas dasar tersebut, penelitian ini mengusulkan model *tiered liability* berbasis kapabilitas. Platform besar dengan pengguna aktif lebih dari 10 juta di Indonesia, seperti Meta, TikTok, YouTube, dan X, diwajibkan menerapkan deteksi *deepfake* secara proaktif, melakukan pelabelan otomatis terhadap konten yang teridentifikasi sebagai *AI-generated*, menyediakan mekanisme pelaporan yang mudah, dan menerbitkan laporan transparansi secara periodik. Platform sedang dengan pengguna 1–10 juta diwajibkan menerapkan *notice and takedown* yang dipercepat, maksimal 24 jam untuk konten *deepfake* yang telah diverifikasi, menyediakan mekanisme pelaporan, dan bekerja sama dalam investigasi. Platform kecil dengan pengguna di bawah 1 juta dapat tunduk pada kewajiban umum *notice and takedown* dengan mempertimbangkan keterbatasan teknologi dan finansial. Model tersebut sejalan dengan prinsip proporsionalitas dalam hukum administrasi sekaligus menghindari pembebanan kewajiban yang sama kepada seluruh platform. Dengan demikian, *safe harbour* tidak dihapus secara keseluruhan, tetapi dikondisikan pada tingkat kehati-hatian yang sebanding dengan kemampuan dan peran platform.

Rekonstruksi tersebut selanjutnya perlu dihubungkan dengan mekanisme perlindungan preventif dan represif sebagaimana dikembangkan dalam teori perlindungan hukum Phillipus M. Hadjon. Pada sisi preventif, platform perlu menerapkan *technical safeguard*, *content provenance* seperti Coalition for Content Provenance and Authenticity (C2PA), *AI content labeling*, serta program literasi digital yang berorientasi pada kelompok rentan. Lim (2013) menunjukkan bahwa masyarakat pedesaan dan kelompok marginal merupakan kelompok yang rentan terhadap disinformasi karena keterbatasan kemampuan verifikasi informasi. Pada sisi represif, korban dapat menggunakan Pasal 35 jo. Pasal 51 UU ITE terhadap pembuat *deepfake*, Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE terhadap penyebar disinformasi, serta Pasal 65 dan Pasal 66 jo. Pasal 68 UU PDP terhadap pelanggaran data biometrik. Jalur perdata dapat menggunakan Pasal 1365 KUH Perdata, sedangkan jalur administratif dapat ditempuh melalui mekanisme pelaporan kepada Komdigi. Tantangan pembuktian melalui *digital forensics* dan *AI forensics*, anonimitas pelaku, serta karakter lintas yurisdiksi sebagaimana dikemukakan Aini & Lubis, (2024) menunjukkan pentingnya penguatan kapasitas aparat penegak hukum.

Tabel 3. *Model Rekonstruksi Tiered Liability dan Perlindungan Hukum*

Tingkat Platform	**Kapasitas/Pengguna**	**Kewajiban Utama**	**Mekanisme Perlindungan**
Platform besar	>10 juta pengguna Indonesia	Deteksi proaktif, *AI labeling*, pelaporan, transparansi	Preventif dan represif
Platform sedang	1–10 juta pengguna Indonesia	*Notice and takedown*	Respons cepat dan

		maksimal 24 jam untuk *deepfake* terverifikasi	investigasi
Platform kecil	<1 juta pengguna Indonesia	*Notice and takedown* standar	Proporsional dengan kemampuan
Seluruh platform	Semua skala	Mekanisme pelaporan dan kepatuhan terhadap hukum	Perlindungan korban
Pemerintah/lembaga pengawas	Nasional	Menetapkan standar deteksi, pengawasan dan sanksi	*Regulatory oversight*
Penegak hukum	Nasional/lintas yurisdiksi	*AI forensics* dan digital forensics	Perlindungan represif
Pengguna	Masyarakat digital	*Tabayyun*, verifikasi, dan pelaporan	Perlindungan kolaboratif

Tabel 4. *Rekonstruksi Kewajiban Platform dalam Regulasi Masa Depan*

Norma yang Diusulkan	**Substansi**	**Tujuan**	**Dasar Argumentasi**
Definisi *deepfake*	Konten AI yang memanipulasi identitas/representasi secara menyesatkan	Kepastian hukum	Prinsip *lex certa*
Mandatory AI labeling	Label nyata, permanen, dan *machine-readable*	Transparansi	EU AI Act dan *sidq*
Deepfake detection	Deteksi proaktif berbasis teknologi terkini	Pencegahan	Perlindungan preventif Hadjon
Content provenance	Jejak asal-usul konten yang dapat diverifikasi	Autentikasi	C2PA
Accessible	Pelaporan mudah	Akses	Perlindungan

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 8 Nomor 1 Oktober 2026
ISSN (Online): 2714-6917
Halaman 6659-6672

reporting	dalam Bahasa Indonesia	keadilan	korban
Transparency reporting	Laporan setiap 6 bulan	Akuntabilitas	Pengawasan publik
User education	Edukasi pengenalan dan pelaporan *deepfake*	Pencegahan	*Hifzh al-'aql*
Sanksi berlapis	Teguran, denda Rp500 juta–Rp10 miliar, pembatasan fitur, hingga pencabutan PSE	Efek kepatuhan	Proporsionalitas
Counter-notification	Hak mengajukan keberatan atas penghapusan	Keseimbangan hak	Due process

Rekonstruksi norma yang ditawarkan menempatkan tanggung jawab platform dalam kerangka *tiered liability*, yaitu kewajiban yang disesuaikan dengan skala, kapabilitas, dan tingkat risiko platform. Model tersebut memungkinkan Indonesia bergerak dari sistem *notice and takedown* yang dominan reaktif menuju sistem perlindungan preventif tanpa membebani seluruh platform secara seragam. Dalam perspektif hukum ekonomi syariah, model ini juga dapat dipertautkan dengan prinsip *maslahah*, *amanah*, *adl*, *hifzh al-'aql*, *hifzh al-mal*, dan *hifzh al-'ird*. Dengan demikian, rekonstruksi hukum tidak hanya menghasilkan kepastian dan efektivitas penegakan hukum, tetapi juga membangun tata kelola digital yang lebih transparan, bertanggung jawab, dan berorientasi pada perlindungan manusia.

D. Penutup

Berdasakan hasil penelitian dapat disimpulkan bahwa perlindungan hukum terhadap disinformasi visual berbasis *Artificial Intelligence* (*deepfake*) di Indonesia telah memiliki dasar melalui UU ITE, UU PDP, PP No. 71 Tahun 2019, dan ketentuan perdata, tetapi belum mengatur *deepfake* secara khusus, terintegrasi, dan adaptif terhadap karakteristik teknologi AI. Dalam perspektif hukum ekonomi syariah, *deepfake* yang digunakan untuk menipu atau merugikan bertentangan dengan prinsip *sidq*, *amanah*, *adl*, larangan *tadlis*, *gharar*, dan *al-kadhib*, serta mengancam *hifzh al-'aql, hifzh al-mal,* dan *hifzh al-'ird*. Oleh karena itu, diperlukan penguatan regulasi melalui definisi operasional *deepfake*, *AI content labeling*, deteksi proaktif, *content provenance*, mekanisme pelaporan, *AI forensics*, literasi digital, serta model *tiered liability* yang menyesuaikan kewajiban platform dengan skala dan kapabilitasnya. Penelitian ini terbatas pada pendekatan kualitatif-normatif sehingga belum menguji secara empiris efektivitas deteksi, kapasitas platform, dan kesiapan aparat penegak hukum; penelitian selanjutnya disarankan melakukan kajian empiris dan komparatif untuk menguji efektivitas model tanggung jawab platform serta merumuskan regulasi AI yang mampu menyeimbangkan perlindungan masyarakat, etika syariah, inovasi teknologi, dan kepastian hukum.

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 8 Nomor 1 Oktober 2026
ISSN (Online): 2714-6917
Halaman 6659-6672

DAFTAR PUSTAKA

Abdullah, F. D., Fathonih, A., & Athoillah, M. (2021). Analisis Kajian Tafsir Ahkam tentang Kedudukan Akad Muamalah pada Lembaga Keuangan Syariah di Indonesia. *Jurnal AT-TAHFIDZ Jurnal Ilmu Al-Qur'an Dan Tafsir*, *3*(1), 64.

Abdullah, F. D., Nurhasanah, A. A., Sulistiyo, B., & Saepudin, D. (2024). Analisis Tujuan dan Manfaat Penelitian Ilmiah dalam Pengembangan Hukum Ekonomi Syariah Perspektif Teoritis dan Aplikatif Analysis of the Goals and Benefits of Scientific Research in the Development of Sharia Economic Law from Theoretical and Applicable Pe. *Jurnal Hukum Ekonomi Syariah Dan Keuangan Islam*, *2*(2), 77.

Aini, N., & Lubis, F. (2024). Tantangan pembuktian dalam kasus kejahatan siber. *Judge: Jurnal Hukum*, *5*(02), 55–63.

Akbar, B. M., Yulia, R., Romdoni, M., Hukum, F., Sultan, U., & Tirtayasa, A. (2026). Urgensi Reformulasi Undang-Undang Informasi dan Transaksi Elektronik terhadap Penyalahgunaan Kecerdasan Buatan Deepfake dalam Perspektif Pembaharuan Hukum Pidana kejahatan , seperti pencemaran nama baik , penipuan , pemerasan , penyebaran Situasi. *ALADALAH : Jurnal Politik, Sosial, Hukum Dan Humaniora*, *4*(2), 1–20.

Al-Ghazali, I. H. (1997). *Al-Mustasfa min 'Ilm al-Usul*. Dar al-Risalah.

Anggito, A., & Setiawan, J. (2018). *Metodologi Penelitian Kualitatif*. CV Jejak.

Annabawi, D. D., Dermawan, R. R., Yudi, R. M., Prayoga, S., & Lampung, U. (2025). Dalam Perspektif Filsafat Hukum Kontemporer. *Jurnal Pendidikan Sejarah Dan Riset Sosial Humaniora*, *5*(2), 443–451.

APJII. (2025). *APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*.

Chesney, B., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, *107*, 1753.

Congress, L. of. (2023). Provisions on Deep Synthesis Technology Enter into Effect. In *Library of Congress*. https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/

DIY, K. (2025). Dittipidsiber Tangkap Pelaku Deepfake Presiden Prabowo dan Pejabat Negara Lainnya. In *Bidhumasdiy*. https://jogja.polri.go.id/polda/tribrata-news/online/detail/dittipidsiber-tangkap-pelaku-deepfake-presiden-prabowo-dan-pejabat-negara-lainnya.html

Fadhila, G. T. Y. N. (2026). Tanggung Jawab Platform Digital dan Perlindungan Hak Korban: Analisis Intermediary Liability di Indonesia. *Media Hukum Indonesia (MHI)*, *4*(1), 458–465.

Fatwa MUI Nomor 24 Tahun 2017 Tentang Hukum Dan Pedoman Bermuamalah Melalui Media Sosial (2017).

Febriani, R., Mary, T., & Pernanda, A. Y. (2022). Sistem Informasi Monitoring Praktik Kerja Lapangan (PKL) Berbasis Web di SMK Negeri 1 Sintuk Toboh Gadang. *Jurnal Pustaka Data (Pusat Akses Kajian Database, Analisa Teknologi, Dan Arsitektur Komputer)*, *2*(2), 95–102. https://doi.org/10.55382/jurnalpustakadata.v2i2.291

Harapan, U. P. (2026). Penyalahgunaan Artificial Intelligence Dalam Kejahatan Dunia Maya Terhadap Manipulasi Konten Asusila. *Lex Stricta : Jurnal Ilmu Hukum*, *5*(1), 125–137. https://doi.org/10.46839/lexstricta.v5i1.1738

Hartono, H., Hendra, M., & Suryadi, M. A. (2026). Analisis Normatif Penyalahgunaan Teknologi Deepfake Dalam Kampanye Politik Digital Sebagai Tindak Pidana Siber Berdasarkan Pasal 28 Ayat (2) Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik (ITE). *Jurnal Ilmiah Muqoddimah: Jurnal Ilmu Sosial, Politik,*

Dan Humaniora, *10*(1), 591–601.

Komdigi, D. J. A. I. (Ditjen A. (2019). Fasilitasi Konten Ilegal, Dirjen Aptika: Platform Didenda 500 Juta Per Konten. In *Komdigi*. https://www.komdigi.go.id/berita/berita-kominfo/detail/fasilitasi-konten-ilegal-dirjen-aptika-platform-didenda-500-juta-per-konten

Kurnia, N., & Astuti, S. I. (2021). Digital literacy in Indonesia: Current State and Challenges. *Journal of Southeast Asian Economies*, *38*(2).

Lim, M. (2013). Many Clicks but Little Sticks: Social Media Activism in Indonesia. *Journal of Contemporary Asia*, *43*(4), 636–657.

Mansari, M. (2026). Metodologi Penelitian Hukum: Normatif, Empiris, dan Teknik Pencarian Literatur Digital. Elfarazy Media Publisher.

Quratuainniza, H. S., & Nurkhaerani, E. (2026). Regulasi Kecerdasan Buatan untuk Mengatasi Penyalahgunaan Deepfake di Indonesia. *ALADALAH : Jurnal Politik, Sosial, Hukum Dan Humaniora*, *4*(1).

Setiawan, M. D., & Babussalam, A. B. (2026). Perlindungan Hukum Atas Pemutusan Relasi Kerja Dalam Gig Economy Menurut Teori Philipus M . Hadjon. *Journal Presumption Of Law*, *8*(1), 59–79.

Sudoyo, W. (2023). Surat Edaran Menkominfo terkait Artificial Intelligence Resmi Dirilis. In *InfoPublik*. https://infopublik.id/kategori/nasional-sosial-budaya/811284/surat-edaran-menkominfo-terkait-artificial-intelligence-resmi-dirilis

Wulandari, S. B., Setiyawati, A., Yulanda, M., Saputra, M. R. P., & Pambudi, S. B. (2025). Menakar Intermediary Liability: Tantangan Platform Digital dalam Mengawasi Deepfake Sexual Content. *Konstitusi: Jurnal Studi Hukum*, *2*(1), 1–12.

Yogyakarta, A. (2026). AI Jadi Senjata Siber, Deepfake Naik 1.400 Persen - Wamen Komdigi Buka Workshop Cybersecurity #13 di Yogyakarta, Sekaligus Luncurkan Digital Talent Hub untuk Desa Wisata DIY 2026. In *BPSDM Komdigi Yogyakarta*. https://bpsdm.komdigi.go.id/upt/yogyakarta/berita-ai-jadi-senjata-siber-deepfake-naik-1-400-persen-wamen-komdigi-buka-worksho-5-88