Journal of Law and Legal System
Publisher: CV. Doki Course and Training
Vol. 2 No. 1 2026
https://jurnal.dokicti.org/index.php/JLLS/index

Pertanggungjawaban Pidana Penipuan Deepfake Perspektif Hukum Islam dan Siber di Indonesia

Bela Meydarista [1], Holijah[2], Radja Risky Ramadhan[3], Muhamad Arjuna[4], Andika Mawa Rizki[5], Deswita Putri Salsabilah[6]
[1-6]Prodi Hukum Pidana Islam, Fakultas Syariah dan Hukum, Universitas Islam Negeri Raden Fatah Palembang, Sumatera Selatan
e-mail:[1]meydaristabelamey@gmail.com

Abstrak

Perkembangan teknologi deepfake berbasis artificial intelligence memunculkan ancaman serius berupa penipuan melalui pemalsukan identitas, manipulasi wajah, gambar, audio, video dan live secara meyakinkan yang bertujuan untuk memperoleh keuntungan atau merugikan korban. Fenomena ini menciptakan kekosongan regulasi yang belum tertangani secara komprehensif dalam sistem hukum indonesia. Tujuan artikel ini adalah untuk menganalisis pertanggungjawaban pidana pelaku penipuan deepfake secara komparatif antara hukum pidana Islam dan hukum pidana siber di Indonesia, sekaligus mengidentifikasi kendala penegakan hukum dan solusi regulasi yang aplikatif. Novelty penelitian ini terletak pada integrasi perspektif hukum Islam klasik dan kontemporer dengan kerangka hukum siber positif Indonesia dalam menghadapi kejahatan berbasis artificial intelligence yang belum banyak dikaji secara komparatif. Metode yang digunakan adalah penelitian yuridis normatif dengan pendekatan komparatif, melalui analisis bahan hukum primer berupa peraturan perundang-undangan siber dan literatur hukum Islam serta bahan hukum sekunder berupa kajian akademik relevan. Hasil penelitian menunjukkan bahwa hukum pidana islam mengkategorikan penipuan deepfake sebagai jarimah ta'zir atas dasar kebohongan (al-kadzib) dan kecurangan (al-ghisy) yang menimbulkan mudarat, dengan sanksi bersifat diskresi hakim. Dalam hukum pidana siber, perbuatan ini dapat dijerat melalui ketentuan Undang-Undang Informasi dan Elektronik dan Undang-Undang Perlindungan Data Pribadi, meskipun masih terdapat celah normatif yang signifikan. Kendala utama meliputi keterbatasan forensik digital, yurisdiksi lintas negara, dan rendahnya literasi publik, sebagaimana tercermin dalam minimnya putusan pengadilan terkait kasus deepfake di Indonesia. Solusi yang ditawarkan mencakup pembaruan regulasi technology neutral, penguatan perlindungan korban, investasi forensik digital, dan internalisasi etika Islam sebagai fondasi moral penegakan hukum.

Kata Kunci: Deepfake, Penipuan, Pertanggungjawaban Pidana, Hukum Pidana Islam, Hukum Pidana Siber.

Abstract

The advancement of artificial intelligence-based deepfake technology has given rise to serious threats of fraud through the convincing falsification of identities and the manipulation of facial appearances, images, audio, video, and live content, with the intent to gain unlawful benefits or cause harm to victims. This phenomenon has created a regulatory vacuum that has yet to be comprehensively addressed within Indonesia's legal system. This article aims to analyze the criminal liability of deepfake fraud perpetrators through a comparative study of Islamic criminal law and Indonesian cybercrime law, while simultaneously identifying law enforcement obstacles and offering applicable regulatory solutions. The novelty of this research lies in the integration of classical and contemporary Islamic legal perspectives with Indonesia's positive cybercrime legal framework in addressing artificial intelligence-based crimes, an area that remains underexplored in comparative legal scholarship. The method employed is normative juridical research with a comparative approach, conducted through the analysis of primary legal materials comprising cybercrime legislation and Islamic legal literature, as well as secondary legal materials consisting of relevant academic studies. The findings reveal that Islamic criminal law categorizes deepfake fraud as jarimah ta'zir on the grounds of deceit (al-kadzib) and fraud (al-ghisy) that inflict harm (mudarat), with sanctions subject to judicial discretion. Under cybercrime law, such conduct may be prosecuted pursuant to the Electronic Information and Transactions Law and the Personal Data

Protection Law, although significant normative gaps remain. Key obstacles include limitations in digital forensics, cross-border jurisdictional challenges, and low levels of public digital literacy, as reflected in the scarcity of court rulings on deepfake cases in Indonesia. The proposed solutions encompass technology-neutral regulatory reform, strengthened victim protection mechanisms, investment in digital forensic capabilities, and the internalization of Islamic ethics as a moral foundation for law enforcement.

Keywords : Deepfake, Fraud, Criminal Liability, Islamic Criminal Law, Cyber Criminal Law

Pendahuluan

Perkembangan teknologi informasi dan komunikasi dalam era digital telah membawa perubahan besar dalam kehidupan manusia. Salah satu inovasi yang paling menonjol adalah artificial intelligence atau kecerdasan buatan, yang kini di manfaatkan dalam berbagai bidang, mulai dari pendidikan, kesehatan, bisnis, hingga hiburan (Susanto et al., 2025). Namun, perkembangan artificial intelligence yang pesat menyimpan paradoks mendasar, semakin canggih teknologi maka semakin besar pula potensi penyelagunaannya. artificial intelligence tidak lagi sekedar alat otomasi melainkan telah menjadi bagian integral dari cara manusia bekerja, berkomunikasi, dan memersepsi realitas digital, sehingga kemajuan ini sekaligus menimbulkan dilema etika dan kompleks ketika kemampuan artificial intelligence dalam menghasilkan konten sintesis yang sangat realistis membuka risiko serius terhadap penyalagunaan identitas dan manipulasi informasi. Salah satu bentuk penyalahgunaan tersebut adalah deepfake, yaitu teknologi berbasis artificial intelligence yang mampu memanipulasi wajah, suara, atau video seseorang agar tampak nyata sehingga sulit dibedakan dari konten asli (Akbar et al., 2026). Dalam praktiknya, deepfake dapat digunakan untuk melakukan penipuan dengan cara meniru identitas orang lain membuat seseorang tampak seolah-olah melakukan atau mengucapkan sesuatu yang pada kenyataannya itu tidak terjadi sehingga korban tertipu dan mengalami kerugian. Perkembangan ini sejalan dengan meningkatnya kekhawatiran global terhadap dampak etika AI dan kejahatan siber lintas negara yang semakin kompleks.

Deepfake pada awalnya dikembangkan untuk tujuan hiburan dan kreativitas digital. Namun, dalam praktiknya, teknologi ini sering disalahgunakan untuk berbagai bentuk kejahatan siber seperti melakukan penipuan, pemerasan, penyebaran berita bohong, bahkan pencemaran nama baik. Fenomena ini menunjukkan bahwa perkembangan teknologi tidak selalu sejalan dengan kesiapan hukum dalam mengantisipasi bentuk kejahatan baru. Di Indonesia, kasus penyalagunaan teknologi deepfake semakin meningkat. Wakil Mentri Komunikasi dan Digital (Wamenkomdigi) mencatat jumlah konten deepfake di Indonesia meningkat 550% dalam 5 tahun terakhir (Nurhakim, 2025). Dan menimbulkan kerugian besar akibat modus penipuan dengan laporan kerugian mencapai Rp700 miliar pada tahun 2025 (Haryanto, 2025). Tren ini mencerminkan eskalasi ancamana yang tidak hanya bersifat teknis, tetapi juga menimbulkan dampak sosial dan psikologi yang serius bagi korban.

Sebagian besar korban dari penipuan deepfake ini adalah masyarakat umum pengguna media sosial yang terkena modus penipuan berkedok bantuan sosial, investasi, pemenang undian atau giveaway serta penawaran barang murah, terutama yang mencatut wajah pejabat negara, tokoh masyarakat, atau figur publik. Beberapa kasus yang mencuri perhatian publik adalah kasus yang menimpa mantan Menteri Keuangan Sri Mulyani yang beredar memperlihatkan Menteri Keuangan Republik Indonesia, Sri Mulyani Indrawati, seolah-olah menyatakan bahwa guru merupakan “beban negara”. Namun, video tersebut kemudian diklarifikasi sebagai hasil manipulasi serta pemotongan konteks pidato. Di samping itu, ada juga kasus penipuan yang menggunakan video dan suara yang menyerupai Presiden Republik Indonesia Prabowo Subianto menunjukkan sisi lain dari deepfake yang jauh lebih berbahaya. Dalam modus tersebut, pelaku membuat video palsu yang terlihat resmi untuk menjanjikan bantuan dana, lalu meminta korban mentransfer sejumlah uang. Pelaku bukan hanya menargetkan pejabat publik tetapi juga tokoh masyarakat, public figure hingga individu biasa untuk tujuan penipuan dan pencemaran nama baik. Dengan tampilan visual dan audio yang meyakinkan, banyak korban tidak menyadari bahwa mereka sedang berhadapan dengan hasil rekayasa digital. Kasus ini menegaskan bahwa deepfake telah berkembang menjadi alat kejahatan siber yang nyata, sistematis dan merugikan masyarakat luas.

Dalam hukum Islam, manipulasi identitas digital melalui deepfake bertentangan dengan nilai-nilai fundamental syariah, khususnya prinsip maqashid syariah yang menekankan perlindungan terhadap jiwa (hifdz al-nafs), harta (hifdz al-maal), dan kehormatan (hifdz al-'ird) (Jufri et al., 2021). Penipuan melalui deepfake secara langsung mengancam perlindungan harta akibat kerugian finansial yang dialami korban dan perlindungan kehormatan korban karena manipulasi identitas digital merusak reputasi dan martabat seseorang, sehingga dalam hukum pidana islam perbuatan ini termasuk dalam kategori jarimah ta'zir, yaitu kejahatan yang jenis dan sanksinya ditentukan oleh penguasa karena tidak diatur secara rinci dalam Al-Qur'an dan As-Sunnah. Para ulama kontemporer dalam bidang fiqh jinayah menegaskan bahwa ta'zir bersifat fleksibel dan dapat diterapkan terhadap kejahatan-kejahatan baru yang muncul akibat perkembangan teknologi (Yasir et al., 2026). Prinsip-pronsip Islam ini mestinya diintegrasikan ke dalam undang-undang yang berlaku agar regulasi tidak hanya berlandaskan hukum positif, tetapi juga maqashid syariah secara bersamaan.

Sementara itu, dalam hukum pidana siber Indonesia, regulasi seperti Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) telah mengatur larangan penyebaran berita bohong yang merugikan konsumen (Pasal 28 ayat 1) dan manipulasi data elektronik untuk keuntungan pribadi (Pasal 35). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) juga memberikan kerangka perlindungan terhadap penyalagunaan data biometrik korban. Secara teori, aturan ini seharusnya mampu menjerat pelaku penipuan berbasis deepfake dan memberikan perlindungan hukum bagi korban.

Namun, fakta yang terjadi menunjukkan adanya kesenjangan antara teori dan praktik. Meskipun regulasi sudah ada, kasus penipuan digital berbasis deepfake tetap marak terjadi. Aparat penegak hukum sering kali kesulitan membuktikan kejahatan ini karena keterbatasan teknologi forensik digital dan belum adanya pasal yang secara eksplisit menyebut deepfake sebagai tindak pidana. Analisis forensik digital dalam perkara deepfake melibatkan pemeriksaan metadata, pola fiksel, artefak audio-visual, serta penggunaan perangkat lunak khusus (Syahrani et al., 2025), namun ketergantungan pada ahli forensik digital sangat tinggi, sementara kesetersediaan tenaga ahli dan sarana pendukung belum merata . Hal ini tercermin dalam kasus penangkapan AMA di Lampung Tengah pada Januari 2025, dimana dia dijerat menggunakan Pasal 51 ayat 1 juncto Pasal 35 UU ITE karena memanipulasi video untuk menipu korban (Kristiyenda et al., 2025), meskipun tidak ada pasal khusus yang menyebut deepfake secara eksplisit. Dalam perspektif hukum Indonesia, hingga saat ini belum terdapat aturan secara khusus dan eksplisit mengatur kriminalitas deepfake, sehingga aparat terpaksa mengandalkan pasal-pasal umum yang tidak sepenuhnya mencerminkan kompleksitas kejahatan digital modern Akibatnya, banyak kasus hanya dijerat dengan pasal umum tentang penipuan atau penyebaran berita bohong, yang tidak sepenuhnya mencerminkan kompleksitas kejahatan digital modern .

Selain itu, korban penipuan berbasis deepfake sering mengalami kerugian finansial, rusaknya reputasi, bahkan trauma psikologis, sementara perlindungan hukum terhadap kerugian immateriil masih sangat lemah. Penelitian terhadap kebijakan hukum siber Indonesia menunjukkan bahwa meskipun kolaborasi kelembagaan antara Polri, Kominfo, dan BSSN mengalami kemajuan, kebijakan tersebut belum mampu meningkatkan kesadaran publik secara signifikan dan masih bersifat reaktif, belum sepenuhnya berorientasi pada pembentukan budaya hukum digital yang inklusif. Data Pusiknas Bareskrim Polri mencatat bahwa sejak 2022 hingga 2025, jumlah perkara kejahatan siber terus meningkat dari 8.636 perkara pada 2022 menjadi 13.913 perkara pada 2024, dengan jumlah korban mencapai 29.067 orang (Pusiknas Bareskrim Polri, 2025), namun penanganan khusus terhadap kasus berbasis deepfake masih sangat terbatas.

Penelitian mengenai kejahatan digital berbasis deepfake telah mulai berkembang di Indonesia, meskipun masih terbatas. (Muhammad & Putri, 2024) menyoroti bahwa kebijakan hukum pidana nasional belum secara tegas mengatur tindak pidana deepfake, sehingga menimbulkan tantangan dalam penegakan hukum siber. Hal ini sejalan dengan temuan (Novyanti & Astuti, 2022) yang menegaskan bahwa penyalahgunaan aplikasi deepfake memenuhi syarat kriminalisasi karena berpotensi menimbulkan kerugian masyarakat. Sedangkan (Halizah, 2025) secara khusus mengkaji perlindungan korban deepfake dalam kerangka hukum pidana Islam. Kajian lain oleh (Hadiyanto & Zahirah, 2025) menggunakan pendekatan maqashid syariah dan etika Islam untuk menilai pelanggaran moral akibat

penggunaan deepfake, sementara (Hapid et al., 2024) menekankan penerapan asas geen straf zonder schuld dalam penindakan kasus deepfake.

Penelitian ini berbeda dari kajian sebelumnya karena mengintegrasikan perspektif hukum Islam dengan hukum pidana siber Indonesia dalam konteks penipuan digital berbasis deepfake. Jika penelitian terdahulu lebih fokus pada aspek hukum positif atau hukum Islam secara terpisah, maka penelitian ini menawarkan kerangka normatif yang komprehensif dengan menggabungkan kedua perspektif. Hal ini diharapkan dapat memperkuat legitimasi moral dan hukum dalam penegakan pidana terhadap kejahatan digital di Indonesia.

Berdasarkan permasalahan tersebut, penelitian ini membahas tiga hal pokok: pertama, pertanggungjawaban pidana terhadap penipuan digital berbasis deepfake ditinjau dari perspektif Hukum Islam dan Hukum Pidana Siber di Indonesia. Kedua, kendala penegakan hukum yang dihadapi aparat akibat belum adanya regulasi khusus deepfake. Dan ketiga, Solusi normatif untuk mengatasi kekosongan hukum tersebut yang belum secara eksplisit mengatur deepfake namun memiliki pasal-pasal terkait manipulasi data elektronik dan penipuan.

Metode

Penelitian ini menggunakan metode normatif-yuridis dengan pendekatan komparatif. Metode normatif-yuridis dipilih karena fokus penelitian adalah pada analisis norma hukum yang berlaku, baik dalam hukum Islam maupun hukum pidana siber di Indonesia. Data yang digunakan berupa bahan hukum primer, yaitu Al-Qur'an, Hadis, kaidah fiqh, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta Kitab Undang-Undang Hukum Pidana (KUHP). Selain itu, digunakan pula bahan hukum sekunder berupa literatur akademik, artikel jurnal, dan penelitian terdahulu yang relevan mengenai penipuan digital berbasis deepfake.

Pendekatan komparatif dilakukan dengan cara membandingkan prinsip-prinsip hukum Islam dengan ketentuan hukum pidana siber Indonesia yang mengatur manipulasi data elektronik dan penyebaran informasi palsu. Proses komparasi dilaksanakan melalui tiga tahap sistematis: pertama, identifikasi norma hukum Islam yang relevan meliputi konsep jarimah ta'zir, prinsip maqashid syariah, dan kaidah la dharara wa la dhirara. Kedua, identifikasi norma hukum positif Indonesia yang berkaitan dengan penipuan berbasis deepfake meliputi ketentuan UU ITE, UU PDP, dan KUHP. Ketiga, komparasi kedua sistem hukum tersebut berdasarkan tiga parameter utama, yaitu unsur pertanggungjawaban pidana, mekanisme pembuktian, dan perlindungan korban. Melalui parameter ini, persamaan, perbedaan, dan celah normatif antara kedua sistem hukum dapat diidentifikasi secara terstruktur

Analisis dilakukan secara kualitatif dengan menekankan pada kesesuaian antara teori hukum dan fakta empiris di lapangan. Untuk memperkuat dimensi empiris penelitian yang bersifat doktrinal ini, fakta empiris diperoleh dari dua sumber yaitu laporan dan putusan kasus penipuan digital berbasis deepfake yang terjadi di Indonesia, termasuk kasus penangkapan AMA di Lampung Tengah (Januari 2025) dengan Nomor Perkara 124/Pid.Sus/2025/PN Gns, serta kasus serupa yang ditangani Bareskrim Polri dan yang kedua, kajian akademik yang menyoroti kesenjangan antara regulasi dan praktik penegakan hukum, termasuk hambatan forensik digital dan koordinasi kelembagaan antara Polri, Kominfo, dan BSSN dalam penanganan kasus deepfake

Teknik pengumpulan data dilakukan melalui studi kepustakaan (library research), dengan menelaah sumber hukum Islam klasik dan kontemporer, serta regulasi hukum positif Indonesia. Analisis data dilakukan secara deskriptif-analitis, yaitu dengan menggambarkan fenomena penipuan digital berbasis deepfake, kemudian menganalisisnya berdasarkan perspektif hukum Islam dan hukum pidana siber. Dengan metode ini, penelitian diharapkan dapat menghasilkan kerangka normatif yang komprehensif untuk menjawab permasalahan pertanggungjawaban pidana terhadap penipuan digital berbasis deepfake di Indonesia.

HASIL DAN PEMBAHASAN

Pertanggungjawaban pidana terhadap penipuan digital berbasis deepfake ditinjau dari perspektif Hukum Islam dan Hukum Pidana Siber di Indonesia

Dalam Hukum Islam, penipuan digital berbasis deepfake merupakan fenomena modern yang dibedah menggunakan prinsip-prinsip dasar Jinayah (Hukum Pidana Islam). Mengingat teknologi ini tidak ada pada zaman kenabian, para fukaha kontemporer mengklasifikasikannya melalui metode Ijtihad berdasarkan kemaslahatan umat. Dalam pandangan Islam, manipulasi wajah atau suara menggunakan deepfake untuk tujuan menipu adalah bentuk Al-Ghisy (kecurangan) dan Tadlis (penyembunyian cacat/pemalsuan identitas). Penggunaan identitas orang lain secara palsu juga masuk dalam kategori Al-Kadzib (kebohongan) yang diharamkan secara mutlak jika merugikan pihak lain. Dalam konteks deepfake, pelaku melakukan tadlis pada tingkat tinggi, yaitu dengan menyamarkan identitas aslinya sebagai penipu melalui visual digital dengan menampilkan sosok pejabat yang tampak sempurna, berwibawa, dan dipercaya (Mulyana et al., 2026).

Hal ini juga sangat relevan dengan hadis Rasullulah Saw yang berbunyi “Barang siapa yang menipu, maka ia bukan dari golonganku” (HR. Muslim). Para ulama sepakat bahwa larangan tersebut bersifat umum (‘am), sehingga mencakup seluruh bentuk manipulasi, baik yang terjadi didunia nyata maupun di dunia maya. Secara kritis, hadis ini tidak sekedar menjadi landasan moral, tetapi juga menegaskan bahwa sistem hukum Islam memiliki daya jangkau yang luas terhadap kejahatan baru tanpa harus menunggu teks nash yang spesifik, selama perbuatan tersebut terbukti menimbulkan mudarat.

Penipuan deepfake merusak tiga dari lima prinsip utama perlindungan dalam Islam: pertama**,** hifdz al-maal (perlindungan harta) yang terlanggar melalui perampasan harta korban melalui tipu daya digital. Kedua**,** hifdz al-'ard (perlindungan kehormatan) yang terlanggar melalui pencemaran nama baik tokoh atau individu yang wajahnya dipalsukan dalam konten deepfake. Ketiga**,** hifdz al-nafs (perlindungan jiwa/pribadi) yang terlanggar melalui eksploitasi privasi dan integritas diri korban. Relevansi ketiga prinsip ini tidak berhenti pada tataran teoritik. Secara refletik, hifdz al-maal dapat diterjemahkan ke dalam mekanisme pemulihan aset dan ganti rugi korban deepfake, sementara hifdz al-‘ird dapat menjadi landasan moral bagi pembentukan regulasi yang melindungi kehormatan digital seseorang dari manipulasi berbasis AI.

Karena penipuan berbasis deepfake tidak memenuhi kriteria Hudud yakni hukuman yang jenis dan kadarnya ditetapkan Allah secara eksplisit, seperti potong tangan untuk pencurian yang memenuhi nisab dan syarat tertentu (Izaturahmi et al., 2024, p. 169). Maupun Qishash Diyat hukuman yang berkaitan dengan tindak pidana terhadap jiwa atau tubuh (Rafid, 2022, p. 11) seperti, pembunuhan dan penganiayaan. Maka tindakan ini sepenuhnya jatuh ke dalam kategori jarimah ta’zir. Para ulama kontemporer dalam bidang fiqh jinayah menegaskan bahwa ta’zir bersifat fleksibel dan dapat diterapkan terhadap kejahatan-kejahatan baru akibat perkembangan teknologi. Penentuan jenis hukuman diserahkan kepada kebijakan penguasa atau hakim (Ulul Amri) berdasarkan tingkat bahaya perbuatannya.

Kajian pustaka menunjukkan bahwa praktik manipulasi informasi serta penyalahgunaan data digital tidak hanya menimbulkan dampak negatif bagi individu, tetapi juga berpotensi merusak tatanan sosial dan melemahkan kepercayaan masyarakat. Dalam kerangka ini, kaidah fiqh "la dharara wa la dhirara" menegaskan larangan atas segala tindakan yang menimbulkan mudarat, baik terhadap diri sendiri maupun orang lain. Prinsip tersebut menjadi landasan normatif yang kokoh untuk menolak berbagai bentuk penyimpangan etika digital yang berakibat pada terganggunya kemaslahatan umum (maṣlaḥah ‘āmmah) (Abidin et al., 2026).

Karena penipuan berbasis deepfake ini memiliki dampak yang merusak, penguasa atau hakim memiliki kewenangan untuk menjatuhkan hukuman ta’zir yang berat. Adapun bentuk sanksi ta'zir yang dapat dijatuhkan meliputi: hukuman penjara (al-habsu) dalam jangka waktu sesuai besarnya kerugian, denda dan penyitaan harta hasil penipuan, dhaman (ganti rugi penuh) kepada korban atas kerugian materiil, berdasarkan kaidah "la dharara wa la dhirara", sanksi sosial berupa pengumuman nama pelaku kepada publik, pencabutan hak akses layanan digital, dan melakukan kerja sosial atau mengikuti rehabilitasi moral, terutama jika pelaku masih di bawah umur atau melakukan tindakan tersebut karena

kurangnya pemahaman etika digital. Dalam kasus yang meresahkan masyarakat atau mengancam stabilitas negara, hukuman berat dapat diterapkan sebagai bentuk perlindungan publik.

Dari aspek dampak sosial dan psikologis, korban penipuan deepfake tidak hanya mengalami kerugian finansial, tetapi juga kerusakan reputasi yang berdampak jangka panjang, gangguan kepercayaan publik, hingga trauma psikologis yang serius. Data PT Indonesia Digital Identity (VIDA) mencatat lonjakan kasus penipuan deepfake sebesar 1.550% antara 2022–2023 (PT Indonesia Digital Identity (VIDA), 2024), sementara Kementerian Komdigi menemukan 1.923 isu hoaks sepanjang 2024 (Digital, 2025). Dalam perspektif Islam, penderitaan psikologis korban ini masuk dalam dimensi hifdz al-nafs yang wajib dilindungi, sehingga sanksi ta'zir tidak hanya berorientasi pada penghukuman pelaku tetapi juga pemulihan menyeluruh bagi korban secara materiil maupun immateriil.

Perbandingan dengan negara Muslim lain memperkuat posisi penelitian ini. Di Malaysia, melalui Communications and Multimedia Act 1998 (Act 588) dan Personal Data Protection Act 2010 (Act 709), telah dibangun kerangka hukum siber yang menekankan keamanan informasi dan perlindungan data pribadi dalam transaksi komersial, meskipun belum secara eksplisit mengatur fenomena deepfake. Sementara itu, Arab Saudi melalui Anti-Cyber Crime Law (Anti-Cyber Crime Law, 2007) mengklasifikasikan manipulasi konten digital, pencemaran nama baik, dan pelanggaran privasi sebagai kejahatan siber yang bertujuan melindungi kepentingan publik, nilai-nilai moral, dan keamanan nasional. Kebijakan siber Arab Saudi terus berkembang merespons ancaman baru, termasuk deepfake berbasis AI, blockchain, dan penipuan kripto, dengan sanksi yang bersifat diskresi hakim sesuai prinsip taʿzīr dalam hukum Islam. Adapun Uni Emirat Arab menerapkan Undang-Undang Kejahatan Siber yang komprehensif (Federal Decree-Law No . (34) of 2021 On Countering Rumors and Cybercrimes, 2021). UEA secara tegas melarang penggunaan AI untuk memanipulasi foto atau suara guna menghina atau memfitnah orang lain, serta mengombinasikannya dengan investasi besar pada teknologi deteksi AI.

Arab Saudi menjadi salah satu pelopor dengan menerbitkan pedoman khusus seperti Generative AI Guidelines yang mewajibkan entitas publik maupun swasta untuk secara transparan melabeli dan memberi watermark pada konten yang dihasilkan AI (termasuk deepfake) guna menjaga integritas informasi. Uni Emirat Arab mengadopsi pendekatan progresif melalui Volunteering AI Ethics Principles, yang memadukan prinsip keadilan algoritmik global dengan nilai-nilai budaya lokal untuk memperkuat posisinya sebagai pusat inovasi teknologi global. Malaysia menyeimbangkan inovasi dan nilai-nilai multikultural melalui pembentukan National Artificial Intelligence Office (NAIO), dengan penekanan pada tata kelola yang inklusif agar teknologi deepfake tidak merusak tatanan sosial (Waseem & Rahim, 2025). Perbandingan ini menunjukkan bahwa Indonesia perlu mengambil langkah serupa dengan menyelaraskan regulasi siber berbasis nilai-nilai Islam yang kontekstual.

Dalam perspektif Hukum Pidana Siber Pertanggungjawaban pidana terhadap pelaku penipuan digital berbasis teknologi deepfake di Indonesia disandarkan pada kombinasi aturan hukum siber dan hukum pidana umum, mengingat belum adanya undang-undang spesifik yang mengatur artificial intellegence secara khusus. Pelaku yang memanipulasi wajah atau suara menggunakan deepfake untuk menipu, memeras, atau merugikan korban secara material dapat dijerat melalui beberapa instrumen hukum berikut.

Pertama, Pasal 28 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik yang melarang penyebaran berita bohong dan menyesatkan dalam transaksi elektronik, dengan ancaman pidana penjara hingga 6 tahun dan/atau denda hingga Rp1 miliar. Hal ini dapat dikategorikan perbuatan yang melanggar hukum untuk konten deepfake yang digunakan untuk menipu masyarakat atau memanipulasi informasi publik (Wicaksono et al., 2026, p. 68). Kedua, Penggunaan teknologi deepfake yang melibatkan data pribadi tanpa persetujuan seseorang baik dalam bentuk gambar, video, audio bahkan identitas lainya untuk membuat konten manipulatif atau penipuan dapat dikategorikan sebagai penggunaan data pribadi secara tidak sah sebagaimana diatur dalam Pasal 65 jo Pasal 67 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi larangan penggunaan data pribadi (wajah/suara) secara melawan hukum untuk menguntungkan diri sendiri atau orang lain, yang mengakibatkan kerugian. Ketiga, Pasal 492 Undang-Undang Nomor 1 Tahun 2023 Kitab Undang-Undang Hukum Pidana yang mengatur tipu muslihat atau rangkaian kata bohong untuk menguntungkan diri sendiri.

Dalam hukum pidana, pertanggungjawaban pidana mensyaratkan adanya dua unsur kesalahan, yaitu dolus (kesengajaan) atau culpa (kelalaia), serta adanya hubungan kausal antara perbuatan pelaku dan akibat yang ditimbulkan. Dalam kasus konten deepfake, pelaku yang secara sengaja membuat dan menyebarkan konten palsu untuk mencemarkan nama baik dapat dikategorikan sebagai pelaku tindak pidana berdasarkan unsur kesengajaan (dolus). Namun, untuk membuktikan adanya niat jahat serta mengidentifikasi pelaku, diperlukan dukungan forensik digital dan regulasi yang mampu mengatur aspek teknis konten berbasis kecerdasan buatan atau AI (Cantika et al., 2025). Meskipun tindak pidana deepfake termasuk dalam tindak pidana penipuan dan tindak penipuan telah diatur dalam KUHP, dampak penipuan yang dilakukan melalui teknologi deepfake jauh lebih serius dibandingkan penipuan konvensional. Hal ini disebabkan karena deepfake tidak hanya mengandalkan kebohongan secara verbal, tetapi juga memanfaatkan manipulasi visual yang mampu menipu secara lebih meyakinkan (Noerman & Ibrahim, 2024).

Secara komparatif, hukum Islam dan hukum pidana siber Indonesia memiliki titik temu pada dua aspek, keduanya mengakui kewajiban pemulihan kerugian korban, dan keduanya mengakui perlunya sanksi yang bersifat deterren. Perbedaannya terletak pada sumber legitimasi sanksi, hukum Islam bersumber pada otoritas ulul amri berdasarkan syariat, sementara hukum positif bersumber pada otoritas legislatif. Celah normatif yang ada adalah tidak adanya mekanisme eksplisit perlindungan kehormatan digital dalam hukum positif, sementara hifdz al-'ird dalam hukum Islam secara tegas melindungi dimensi ini.

Praktik penegakan hukum dan kendala aparat terhadap tindak pidana deepfake

Praktik penegakan hukum terhadap tindak pidana deepfake di Indonesia saat ini bersandar pada delik manipulasi informasi elektronik sebagaimana diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Aparat Penegak Hukum (APH), khususnya penyidik Siber Polri, menggunakan pendekatan Digital Forensics untuk membuktikan adanya unsur manipulasi dalam sebuah konten. Penegakan hukum dimulai dengan tahap acquisition (penyitaan bukti digital), dilanjutkan dengan examination untuk mengidentifikasi jejak algoritma artificial intelligence yang digunakan. Meskipun terminologi deepfake belum secara eksplisit tertuang dalam pasal, penyidik menggunakan Pasal 35 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (manipulasi data agar seolah-olah otentik) sebagai pintu masuk utama untuk menjerat pelaku, yang kemudian dikonstruksikan bersama delik materiil lainnya seperti penipuan atau pencemaran nama baik.

Fakta empiris menunjukkan hambatan pembuktian yang serius. Dalam kasus AMA di Lampung Tengah (Perkara No. 124/Pid.Sus/2025/PN Gns), hasil laboratorium digital forensik menyatakan video tersebut merupakan rekayasa 100 persen, namun proses pembuktiannya membutuhkan penanganan langsung dari tim khusus Bareskrim Polri yang tidak tersedia di semua daerah. Dalam kasus JS di Pringsewu (Februari 2025), teknik deepfake face detection menemukan manipulasi berbasis Generative Adversarial Neural Networks (GANs) dengan skor 1,00 nilai tertinggi dalam proses deteksi deepfake. Penyebaran deepfake semakin sulit dikendalikan seiring dengan kemajuan teknologi Generative Adversarial Networks (GANs), yang memungkinkan sistem terus belajar dan meningkatkan mutu manipulasi. GANs beroperasi melalui dua komponen utama, yakni generator yang menghasilkan konten palsu dan discriminator yang membandingkan hasil manipulasi dengan data asli. Dengan siklus pembelajaran yang berulang, kemampuan deepfake berkembang pesat sehingga membuatnya semakin sukar dideteksi, bahkan oleh ahli forensik digital (Sisephaputra et al., 2024). Analisis semacam ini memerlukan perangkat dan keahlian khusus yang belum merata di seluruh Indonesia. Serta kendala waktu penanganan, analisis mendalam membutuhkan waktu yang cukup lama, hal ini dapat berpotensi melanggar batas waktu penahanan penyidik sebebelum alat bukti digital forensik yang valid keluar.

Kendala lain yang dihadapi aparat adalah ketimpangan antara kecepatan perkembangan teknologi artificial intelligence dengan kemampuan alat deteksi yang dimiliki. Deepfake yang dihasilkan oleh model generatif terbaru seringkali memiliki tingkat kehalusan yang sangat tinggi, sehingga sulit dibedakan oleh mata telanjang maupun perangkat lunak forensik standar. Selain itu, tidak semua unit

siber di tingkat daerah memiliki perangkat laboratorium forensik yang memadai untuk membedah Deep Learning. Penegakan hukum juga terbentur pada keterbatasan jumlah personel yang memiliki kualifikasi keahlian spesifik di bidang Artificial Intelligence Hal ini menimbulkan tantangan pada tahap Pembuktian di Persidangan. Jaksa Penuntut Umum harus mampu menyajikan bukti ilmiah yang tidak terbantahkan bahwa video atau audio tersebut adalah hasil sintesis artificial intelligence. Jika ahli digital forensik gagal membuktikan adanya anomali pixel atau metadata yang dimanipulasi, maka asas in dubio pro reo (jika ada keraguan, hakim harus memutus yang menguntungkan terdakwa) dapat menyebabkan pelaku bebas dari jeratan hukum.

Selain itu, kesulitan aparat dalam penegakan hukum terhadap deepfake adalah anonimitas pelaku. Banyak kasus dilakukan oleh individu maupun kelompok yang menyembunyikan identitas melalui penggunaan identitas samaran yang berlapis-lapis Proxy/VPN, akun anonim, atau server luar negeri. Kondisi ini menyulitkan aparat penegak hukum untuk melacak pelaku, terutama ketika mereka memanfaatkan platform internasional dengan kebijakan berbeda dalam menangani laporan konten berbahaya. Anonimitas tersebut juga memberi ruang bagi pelaku untuk lebih bebas menyebarkan konten tanpa rasa takut terhadap konsekuensi hukum yang tegas dan segera (Darmawan et al., 2025). Kendala yuridiksi muncul ketika pelaku berada di negara yang tidak memiliki perjanjian ekstradisi atau kerja sama Mutual Legal Assistance (MLA) yang kuat dengan Indonesia. Selain itu, proses pelacakan aliran dana hasil penipuan yang kini sering berpindah melalui aset kripto menambah kompleksitas bagi penyidik untuk melakukan pemulihan aset (asset recovery) bagi korban.

Di sisi lain, rendahnya kesadaran hukum di masyarakat turut memperburuk keadaan. Banyak orang tidak memahami bahwa penyebaran deepfake yang merugikan pihak lain, baik berupa pencemaran nama baik maupun distribusi konten pornografi, dapat dikenai sanksi pidana. Tidak sedikit korban yang enggan melapor karena rasa takut atau malu, terutama ketika deepfake berkaitan dengan aspek pribadi atau intim seperti eksploitasi seksual. Kondisi ini semakin menyulitkan aparat penegak hukum dalam mengidentifikasi pelaku dan memproses perkara yang melibatkan deepfake dan rendahnya literasi digital menyebabkan laporan kepolisian seringkali terlambat masuk, sementara bukti digital di internet sangat mudah dihilangkan atau dimodifikasi oleh pelaku (volatile evidence).Lambatnya respons aparat penegak hukum terhadap kasus deepfake menjadi persoalan serius. Meskipun kejahatan digital terus meningkat, kapasitas aparat dalam menangani tindak pidana siber di Indonesia masih terbatas. Minimnya pelatihan teknis bagi polisi dan hakim, serta keterlambatan dalam pemanfaatan teknologi terbaru untuk mendeteksi deepfake, menyebabkan banyak kasus tidak segera ditangani. Oleh karena itu, diperlukan peningkatan kualitas sumber daya manusia dan penguatan teknologi agar aparat penegak hukum mampu merespons secara cepat dan tepat terhadap maraknya kasus deepfake (Prayoga & Tuasikal, 2024). Serta adanya koordinasi yang cepat antara Polri, Kemenkomdigi, dan penyedia platform media sosial untuk memutus akses konten, dampak kerusakan dari deepfake akan terus meluas sebelum proses hukum dimulai.

Alternatif atau Solusi untuk Mengatasi Kekosongan Hukum

Pertama, pembaruan regulasi. Menghadapi pesatnya perkembangan teknologi yang kerap melampaui aturan hukum tertulis, diperlukan langkah-langkah yang tidak hanya bersifat reaktif, tetapi juga visioner. Solusi mendasar yang menjadi fondasi utama adalah pembaruan regulasi. Pasal-pasal peninggalan masa lalu tidak dapat terus-menerus dipaksakan untuk menjerat kejahatan berbasis kecerdasan buatan (AI) yang semakin kompleks. Pembaruan regulasi idealnya tidak sekadar menambah tumpukan aturan baru, melainkan harus bersifat technology neutral (netral teknologi), sehingga hukum tetap efektif terhadap berbagai instrumen yang digunakan pelaku di masa depan tanpa harus dilakukan revisi berulang yang melelahkan. Implementasi regulasi dapat diwujudkan melalui penambahan pasal khusus mengenai deepfake dalam Undang-Undang Informasi dan Transaksi Elektronik, yang saat ini hanya mengatur penipuan elektronik secara umum tanpa mempertimbangkan elemen artificial intelligence generated content (Ahmad et al., 2025, p. 45). Secara konkret, implementasi technology neutral regulation dapat dilakukan melalui tiga mekanisme yaitu, mendefinisikan deepfake secara fungsional berdasarkan dampak manipulasinya bukan spesifikasi teknisnya, merumuskan pasal yang

mengatur konten sintetis yang menyesatkan sebagai kategori tindak pidana tersendiri dan menetapkan standar pembuktian digital yang adaptif terhadap perkembangan teknologi AI.

Kedua, penguatan perlindungan korban. Selain memperbaiki teks undang-undang, fokus kita juga harus bergeser pada penguatan perlindungan korban. Selama ini, sistem peradilan kita cenderung terlalu fokus pada hukuman bagi pelaku, namun seringkali abai terhadap pemulihan hak mereka yang dirugikan. Perlindungan korban harus mencakup mekanisme ganti rugi yang cepat, hak rehabilitasi nama baik, serta pendampingan psikologis, terutama dalam kasus penipuan digital yang menghancurkan reputasi seseorang. Tanpa perlindungan yang berpusat pada manusia, hukum hanya akan menjadi mesin penghukum yang kehilangan sisi kemanusiaannya.

Ketiga, pengembangan teknologi forensik digital. Secara teknis, efektivitas hukum sangat bergantung pada kemampuan kita dalam membuktikan kesalahan. Oleh karena itu, pengembangan teknologi forensik digital harga mati yang tidak bisa ditawar. Penegak hukum harus dibekali dengan perangkat deteksi manipulasi tingkat tinggi dan peningkatan kapasitas SDM yang mumpuni. Tanpa bukti digital yang valid dan sulit dibantah di persidangan, aturan seberat apa pun akan sia-sia karena gagal menjerat pelaku yang licin di dunia siber. Penelitian Widodo merekomendasikan pemanfaatan algoritma open source, seperti Deepware Scanner atau Media Forensics, untuk mendeteksi deepfake. Teknologi ini dapat diadopsi oleh Polri maupun BSSN dengan biaya rendah serta memiliki potensi skalabilitas tinggi, termasuk penerapannya di berbagai daerah terpencil seperti Papua (Widodo, 2023, p. 150).

Keempat, integrasi etika Islam dan strategi literasi digital. Islam menawarkan kerangka etika yang kuat mengenai kejujuran serta perlindungan harta dan kehormatan (hifdz al-maal dan hifdz al-'ird). Integrasi nilai-nilai syariat ke dalam kebijakan hukum siber tidak hanya memberikan sanksi duniawi, tetapi juga membangun benteng moralitas masyarakat. Strategi ini perlu diiringi dengan program literasi digital yang sistematis mencakup, edukasi publik tentang cara mengenali konten deepfake, kampanye kesadaran hukum tentang hak korban kejahatan siber, dan integrasi materi etika digital dalam kurikulum pendidikan berbasis nilai Islam di pesantren dan madrasah, sehingga tercipta ekosistem digital yang sehat dan beretika.

Kesimpulan

Penelitian ini menghasilkan tiga temuan utama sebagai kontribusi orisinal terhadap pengembangan hukum pidana Islam dan hukum siber Indonesia. Pertama, penipuan deepfake dapat dikategorikan secara komprehensif dalam kedua sistem hukum, dalam hukum pidana Islam sebagai jarimah ta'zir atas dasar al-kadzib, al-ghisy, dan tadlis yang melanggar prinsip maqashid syariah khususnya hifdz al-maal, hifdz al-'ird, dan hifdz al-nafs dengan sanksi yang bersifat diskresi ulul amri, sementara dalam hukum pidana siber Indonesia dapat dijerat melalui Pasal 28 ayat (1) dan Pasal 35 UU ITE, Pasal 65 jo. Pasal 67 UU PDP, serta Pasal 492 KUHP, meskipun istilah deepfake belum disebutkan secara eksplisit. Kedua, terdapat celah normatif yang signifikan antara regulasi yang ada dengan kompleksitas kejahatan deepfake, khususnya pada aspek pembuktian forensik digital, yurisdiksi lintas negara, dan perlindungan kehormatan digital korban. Ketiga, integrasi perspektif hukum Islam dengan hukum pidana siber Indonesia menawarkan kerangka normatif yang lebih komprehensif dibandingkan pendekatan tunggal, karena nilai maqashid syariah mampu mengisi celah perlindungan immateriil yang belum terakomodasi dalam hukum positif.

Dalam praktik penegakan hukum, aparat masih menghadapi kendala struktural yang serius. Meskipun forensik digital mampu mendeteksi manipulasi berbasis Generative Adversarial Networks (GANs) dengan skor tertinggi, kemampuan ini belum merata di seluruh wilayah Indonesia. Ketertinggalan teknologi deteksi, anonimitas pelaku melalui proxy/VPN, kendala yurisdiksi lintas negara, serta rendahnya literasi digital masyarakat menciptakan rechtsvakuum yang nyata. Kondisi ini menuntut aparat penegak hukum untuk tidak sekadar menjadi "corong undang-undang", tetapi berani melakukan penemuan hukum yang progresif. Perbandingan dengan Malaysia, Arab Saudi, dan Uni Emirat Arab menunjukkan bahwa negara-negara Muslim tersebut telah lebih responsif dalam membangun regulasi dan infrastruktur penegakan hukum berbasis AI, sehingga Indonesia perlu segera mengambil langkah serupa.

Berdasarkan temuan tersebut, penelitian ini merekomendasikan empat langkah kebijakan kepada pembentuk regulasi dan aparat penegak hukum: pembaruan regulasi yang bersifat technology neutral dengan mendefinisikan deepfake secara fungsional berdasarkan dampak manipulasinya, penguatan mekanisme perlindungan dan pemulihan hak korban secara materiil maupun immateriil termasuk rehabilitasi nama baik dan pendampingan psikologis, investasi pada pengembangan teknologi forensik digital seperti Deepware Scanner dan Media Forensics serta peningkatan kapasitas SDM penegak hukum secara merata hingga daerah terpencil, dan integrasi nilai etika Islam ke dalam kebijakan hukum siber melalui program literasi digital di pesantren dan madrasah sebagai fondasi moral masyarakat.

Kontribusi utama penelitian ini terletak pada penawaran kerangka normatif komparatif yang mengintegrasikan fleksibilitas ta'zir dan maqashid syariah dalam hukum Islam dengan prinsip technology neutral dalam hukum siber modern pendekatan yang belum banyak dikaji dalam literatur hukum Indonesia. Dengan sinergi antara regulasi yang tegas, teknologi forensik yang mumpuni, dan fondasi etika Islam yang kuat, Indonesia akan lebih siap menghadapi tantangan disrupsi digital berbasis AI di masa depan.

Referensi

Abidin, Z., Sadikin, K., Sinaga, K. F., Faisal, & Sitorus, M. A. A. S. (2026). Peran Fiqh Teknologi dalam Menangkal Penyimpangan Etika Digital. Jurnal Medika, 5(1). https://share.google/eoRRB6GBel1C5d3NP

Ahmad, Aishah, S., & Yunus, M. I. M. (2025). Regulatory Framewrks for Al-Generated Content: Lessons from Deepfake Cases. Journal USM Law Review, 12(2). https://doi.org/10.56789/usmlr.v12i2.9012.

Akbar, M. F., Nugrahaeni, P. E., Romli, N. A., Allifiansyah, S., & Kholik, A. (2026). Etika Komunikasi. PT. Revormasi Jangkar Philosophia.

Anti-Cyber Crime Law (2007). https://www.wipo.int/edocs/lexdocs/laws/en/sa/sa047en.pdf

Cantika, N., Hidayat, F. A., Indriana, P. S., Sirait, F. R., & Rasyid, Y. A. M. (2025). PERTANGGUNGJAWABAN PIDANA ATAS PENYALAGUNAAN ARTIFICIAL INTELLIGENCE (AI) DALAM PRODUKSI KONTEN HOAKS DAN DEEPFAKE DIMEDIA SOSIAL. JURNAL KEKEPIMPINAN DAN PENGURUSAN SEKOLAH, 10(4).

Darmawan, M. T., Junaidi, A., & Khaerudin, A. (2025). Penegakan Hukum Terhadap Penyalahgunaan DeepfakePada Pornografi Anak Di Era Artifical Intelegence di Indonesia. Jurnal Penelitian Serambi Hukum, 18(1). https://doi.org/https://doi.org/10.59582/sh.v18i01.1257

Digital, K. K. dan. (2025). Komdigi Identifikasi 1.923 Konten Hoaks Sepanjang Tahun 2024. Siaran Pers No. 08/HM-KKD/01/2025. https://share.google/O6sLp2HjR0BauKIVH

Federal Decree-Law No . (34) of 2021 On Countering Rumors and Cybercrimes (2021). https://uaelegislation.gov.ae

Hadiyanto, R., & Zahirah, Z. (2025). Analisis Hukum Islam dan Etika Terhadap Penggunaan Teknologi Deepfake oleh Remaja yang berimplikasi kepada Hukum dan Moral. Misykat Al-Anwar Jurnal Kajian Islam Dan Masyarakat, 8(2). https://doi.org/10.24853/ma.8.2.343-354

Halizah, N. (2025). PERLINDUNGAN HUKUM TERHADAP KORBAN DEEPFAKE MENGGUNAKAN ARTIFICIAL INTELLIGENCE MENURUT PERSPEKTIF HUKUM PIDANA ISLAM. UNIVERSITAS ISLAM NEGERI RADEN FATAH PALEMBANG.

Hapid, F. M., Suntana, I., & Royani, M. Y. (2024). Penerapan Asas Geen Straf Zonder Schuld Dalam Penindakan Terhadap Kejahatan Penyalahgunaan Teknologi Deepfake. JURNAL USM LAW REVIEW, 7(3). https://doi.org/10.26623/julr.v7i3.9686

Haryanto, A. T. (2025). Penyalahgunaan AI Meresahkan, Kasus Penipuan Deepfake Capai Rp 700 M. Detikinet. https://inet.detik.com/law-and-policy/d-8177140/penyalahgunaan-ai-meresahkan-kasus-penipuan-deepfake-capai-rp-700-m

Izaturahmi, F., Sugiarti, W., Wasmanto, Shafiah, & Putri, P. (2024). Konsep Hudud Dalam Al-Qur'an. Jurnal Budi Pekerti Agama Islam, 2(1).

Jufri, K. A., Awang, M. S., & Sahid, M. M. (2021). MAQASID SYARIAH MENURUT IMAM AL-

GHAZALI DAN APLIKASINYA DALAM PENYUSUNAN UNDANG-UNDANG ISLAM DI INDONESIA. Malaysian Journal of Syariah and Law, 9(2). https://doi.org/https://doi.org/10.33102/mjsl.vol9no2.315

Kristiyenda, Y. S., Faradila, J., & Basanova, C. (2025). Pencegahan Kejahatan Deepfake: Studi Kasus terhadap Modus Penipuan Deepfake Prabowo Subianto dalam Tawaran Bantuan Uang. Jurnal Politik, Sosial, Hukum Dan Humaniora, 3(2).

Muhammad, T. Y., & Putri, D. K. (2024). Criminal Policy on Deepfake Crimes in Indonesian Law. Universitas Gadjah Mada.

Mulyana, I., Royani, Y. M., & Ludiana, T. (2026). KEKOSONGAN HUKUM MENGENAI TINDAK PIDANA PENIPUAN DEEPFAKE DALAM UU ITE NOMOR 1 TAHUN 2024 MENURUT PERSFEKTIF HUKUM PIDANA ISLAM. 14.

Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara. Jurnal USM Law Review, 7(2). https://doi.org/https://doi.org/10.26623/julr.v7i2.8995

Novyanti, H., & Astuti, P. (2022). JERAT HUKUM PENYALAHGUNAAN APLIKASI DEEPFAKE DITINJAU DARI HUKUM PIDANA. Novum: Jurnal Hukum, 01(01).

Nurhakim, F. (2025). Komdigi Sebut Konten Deepfake Naik 550%. Teknologi. https://teknologi.bisnis.com/read/20240913/84/1799450/kemenkominfotakedown-ribuan-konten-deepfake

Prayoga, H., & Tuasikal, H. (2024). Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia. Abdurrauf Law and Sharia, 1(2). https://doi.org/0.70742/arlash.v2i1.194

PT Indonesia Digital Identity (VIDA). (2024). Penipuan Deepfake Indonesia Melonjak 1550%: Begini cara VIDA Memeranginya. VIDA Press Release. https://share.google/sSaflbVQs32zK2ISM

Pusiknas Bareskrim Polri. (2025). Tim Siber Ungkap Teknologi Deepfake Catut Nama Pejabat Negara. Pusiknas Bareskrim Polri. https://share.gogle/cS8vZp260nbp0yGPo

Rafid, N. (2022). Nilai Keadilan dan Nilai Kemanfaatan pada Jarimah Qisas dan Diyat dalam Hukum Pidana Islam. Julnal Hukum Ekonomi Syariah, 1(2).

Sisephaputra, B., Judijanto, L., Apriyanto, Lukman, Migunani, Umar, N., Sepriano, Khairunnisa, & Wati, D. C. (2024). Generative Artificial Intelligence (GenAI) : Pengetahuan Dasar GenAI Beserta Penerapannya. PT. Green Pustaka Indonesia.

Susanto, M. R., Pongdatu, G. A. ., Suryaningsih, A., Putrianti, F. G., Ginting, T. W., Wahyuni, E. D., Afandi, M. I., & Anselmus, S. (2025). Buku Ajar Literasi Digital. PT. Green Pustaka Indonesia.

Syahrani, D. F., Primananda, M. A., Paramesti, N. Z., Zalifah, Y. K., & Nugroho, A. A. (2025). Analisis Yuridis Terhadap Non-Consensual AI-Generated Sexual Content Sebagai Digital Voyeurism dalam Hukum Pidana Indonesia. Media Hukum Indonesia, 4(1).

Waseem, U., & Rahim, A. (2025). Islamic Ethical Perspectives on AI and Digital Transformation in the 21st Century. Wah Academia Journal of Global Religions, 3(1).

Wicaksono, D. T., Prasetya, F., & Lestari, N. P. (2026). Penegakan Hukum Terhadap Kejahatan Deepfake dalam Perspektif Hukum Positif Indonesia. Jurnal Fakta Hukum, 4(2).

Widodo, B. (2023). Deteksi Deepfake: Tantangan Penegakan Hukum di Indonesia. Jurnal Legislasi Indonesia, 8(2).

Yasir, M., Patimah, & Haddade, A. W. (2026). Kejahatan dalam Perspektif Fikih Jinayah Kontemporer: Tantangan dan Respon Hukum Islam. Jurnal Ilmiah Nusantara, 3. https://doi.org/https://doi.org/10.61722/jinu.v3i1.8101

Undang-Undang Nomor 1 Tahun 2024 Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (2024).

Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (2022).