

PERLINDUNGAN HUKUM TERHADAP PENYALAHGUNAAN *DEEFAKE* BERBASIS KECERDASAN BUATAN DI INDONESIA

Diana Sari^{1*}, Destri Natalia²

^{1,2}Universitas Islam Nusantara Al-Azhaar Lubuklinggau, Indonesia

*Correspondence: e-mail: dsari0945@gmail.com

Abstract

The development of artificial intelligence (AI) has introduced *deepfake* technology, which can realistically generate or manipulate images, voices, and videos of individuals. Although this technology may serve creative and educational purposes, its misuse can lead to privacy violations, identity manipulation, fraud, defamation, and the non-consensual distribution of intimate content. This study aims to analyze legal protection for victims of *deepfake* misuse in Indonesia, examine the legal liability of perpetrators, and identify challenges in law enforcement. The research employs a normative legal method using statutory and conceptual approaches. Legal materials are analyzed qualitatively through an examination of relevant legislation and legal literature. The study indicates that victim protection may be examined through constitutional provisions, electronic information and transaction laws, personal data protection legislation, and relevant criminal and civil law provisions. Their application, however, requires proof of the relevant legal elements and cannot be based solely on the use of *deepfake* technology. Challenges include digital evidence authentication, perpetrator identification, cross-platform content distribution, and victim redress. Strengthening complaint mechanisms, digital forensic capacity, law enforcement coordination, and regulatory evaluation is therefore necessary to improve legal certainty and victim protection.

Keywords: *deepfake*, artificial intelligence, criminal law.

Abstrak

Perkembangan teknologi kecerdasan buatan (Artificial Intelligence/AI) telah menghadirkan teknologi *deepfake* yang mampu menghasilkan atau memanipulasi gambar, suara, dan video seseorang secara realistis. Penggunaan teknologi tersebut dapat memberikan manfaat dalam bidang kreatif dan pendidikan, tetapi penyalahgunaannya berpotensi menimbulkan pelanggaran privasi, manipulasi identitas, penipuan, pencemaran nama baik, dan penyebaran konten intim tanpa persetujuan. Penelitian ini bertujuan untuk menganalisis perlindungan hukum terhadap korban penyalahgunaan *deepfake* di Indonesia, mengkaji

pertanggungjawaban hukum pelaku, serta mengidentifikasi kendala penegakan hukum. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan konseptual. Bahan hukum dianalisis secara kualitatif melalui penelaahan terhadap peraturan perundang-undangan dan literatur hukum yang relevan. Hasil kajian menunjukkan bahwa perlindungan terhadap korban dapat ditelaah melalui ketentuan konstitusional, hukum informasi dan transaksi elektronik, perlindungan data pribadi, serta ketentuan pidana dan perdata yang relevan dengan perbuatan konkret. Namun, penerapannya memerlukan pembuktian terhadap unsur hukum yang bersangkutan dan tidak dapat didasarkan semata-mata pada penggunaan teknologi *deepfake*. Kendala yang dihadapi meliputi autentikasi bukti digital, identifikasi pelaku, penyebaran konten lintas platform, dan pemulihan hak korban. Oleh karena itu, diperlukan penguatan mekanisme pengaduan, kapasitas forensik digital, koordinasi penegakan hukum, dan evaluasi regulasi untuk meningkatkan kepastian hukum serta perlindungan korban.

Kata kunci: *deepfake*, kecerdasan buatan, hukum pidana.

PENDAHULUAN

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam kehidupan masyarakat. Kemajuan kecerdasan buatan memungkinkan berbagai pekerjaan yang sebelumnya memerlukan keterampilan teknis tinggi dilakukan secara lebih mudah, termasuk pembuatan gambar, suara, dan video sintesis. Salah satu teknologi yang berkembang dalam konteks tersebut adalah *deepfake*. *Deepfake* merupakan konten digital yang dihasilkan atau dimanipulasi dengan bantuan teknologi kecerdasan buatan sehingga menyerupai wajah, suara, gerakan, atau penampilan seseorang (Akhtar, 2024). Teknologi ini dapat digunakan dalam produksi film, hiburan, pendidikan, dan berbagai kegiatan kreatif. Akan tetapi, penggunaannya juga dapat menimbulkan persoalan hukum apabila dilakukan untuk menipu, merusak reputasi, memanipulasi identitas, atau menyebarkan konten pribadi tanpa persetujuan.

Penyalahgunaan *deepfake* dapat menempatkan seseorang seolah-olah melakukan atau mengucapkan sesuatu yang sebenarnya tidak pernah dilakukan atau disampaikan. Konten semacam ini berpotensi memengaruhi persepsi masyarakat terhadap korban. Ketika konten tersebar melalui media sosial, korban dapat mengalami kesulitan mengendalikan distribusi dan mencegah munculnya salinan baru (Wirasmara, 2026). Dampak penyalahgunaan *deepfake* tidak terbatas pada kerugian ekonomi. Manipulasi identitas juga dapat memengaruhi kehormatan, privasi, rasa aman, dan kehidupan sosial korban.

Dalam kasus tertentu, korban dapat menghadapi penyebaran konten intim palsu yang menimbulkan kerugian serius terhadap martabat dan kehidupan pribadinya.

Dalam sistem hukum Indonesia, perlindungan terhadap korban dapat dikaji melalui beberapa instrumen hukum. Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 memberikan dasar perlindungan terhadap diri pribadi, kehormatan, martabat, dan rasa aman. Sementara itu, Undang-Undang Nomor 1 Tahun 2024 merupakan perubahan kedua atas Undang-Undang Informasi dan Transaksi Elektronik, dan Undang-Undang Nomor 27 Tahun 2022 mengatur Pelindungan Data Pribadi. Meskipun di Indonesia tidak memiliki regulasi khusus yang mengatur penyalahgunaan *deepfake* berbasis kecerdasan buatan, sehingga perlindungan hukum bagi korban masih bersifat parsial dan tersebar across beberapa undang-undang yang tidak dirancang untuk media sintetik AI (Seveny,2025).

Kerangka hukum yang ada –UU ITE, UU Pornografi, UU Perlindungan Data Pribadi, dan KUHP hanya sebagian menjawab tantangan *deepfake* dan menciptakan ketidakpastian hukum dalam penegakan (Oscar, 2026). Namun, sejumlah peraturan dapat digunakan untuk menangani perbuatan yang berkaitan dengan *deepfake*, penerapannya perlu dilakukan secara cermat. Tidak semua penggunaan *deepfake* merupakan tindak pidana. Penentuan pertanggungjawaban hukum harus didasarkan pada bentuk perbuatan, unsur ketentuan yang digunakan, kesalahan pelaku, dan bukti yang tersedia.

Kajian mengenai *deepfake* juga telah berkembang dalam literatur hukum Indonesia. Penelitian Fitriani dan Wahyudi (2026), misalnya, membahas kebijakan formulasi tindak pidana *deepfake* dalam UU ITE dan UU PDP. Kajian lain pada 2026 menelaah perlindungan korban melalui pendekatan keadilan yang berorientasi pada korban. Perkembangan penelitian tersebut memperlihatkan pentingnya pembahasan mengenai penerapan perlindungan hukum dalam kasus konkret, termasuk pembuktian dan pemulihan hak korban. Berdasarkan latar belakang tersebut, penelitian ini mengkaji perlindungan hukum terhadap penyalahgunaan *deepfake* berbasis kecerdasan buatan di Indonesia dengan menitikberatkan pada keterkaitan antara peraturan yang berlaku, pertanggungjawaban hukum, serta kendala penegakan hukum.

Penelitian ini bertujuan untuk menganalisis pengaturan perlindungan hukum terhadap korban penyalahgunaan *deepfake*, mengkaji pertanggungjawaban

hukum pelaku berdasarkan ketentuan yang relevan, serta mengidentifikasi upaya penguatan perlindungan korban dalam menghadapi perkembangan teknologi kecerdasan buatan.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu penelitian yang mengkaji norma hukum, asas hukum, dan peraturan perundang-undangan yang berkaitan dengan permasalahan hukum. Pendekatan yang digunakan adalah pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan dengan menelaah peraturan yang berkaitan dengan hak konstitusional, informasi elektronik, perlindungan data pribadi, dan pertanggungjawaban hukum (Widyanto, 2026).

Pendekatan konseptual digunakan untuk mengkaji konsep perlindungan hukum, hak privasi, pertanggungjawaban pidana, dan pemulihan hak korban. Bahan hukum primer meliputi UUD Negara Republik Indonesia Tahun 1945, Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Pelindungan Data Pribadi, Kitab Undang-Undang Hukum Pidana, serta peraturan lain yang relevan dengan bentuk penyalahgunaan yang dikaji. Bahan hukum sekunder meliputi buku hukum, artikel jurnal ilmiah, dan hasil penelitian yang berkaitan dengan *deepfake*.

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan. Bahan hukum yang diperoleh kemudian dianalisis secara kualitatif dengan mengidentifikasi norma yang relevan, menafsirkan unsur hukum, dan menghubungkannya dengan karakteristik penyalahgunaan *deepfake*.

HASIL DAN PEMBAHASAN

Perlindungan Hak Konstitusional

Perlindungan hukum terhadap korban penyalahgunaan *deepfake* dapat dikaitkan dengan hak konstitusional warga negara. Pasal 28G ayat (1) UUD Negara Republik Indonesia Tahun 1945 menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan. Ketentuan tersebut relevan ketika teknologi *deepfake* digunakan untuk memanipulasi identitas atau menyebarkan konten yang merugikan kehormatan dan privasi seseorang. Hak atas

perlindungan diri pribadi memberikan landasan penting bagi pengembangan mekanisme hukum yang melindungi individu dari penyalahgunaan teknologi digital. Namun, ketentuan konstitusional tersebut perlu dihubungkan dengan peraturan pelaksana dan mekanisme hukum yang sesuai. Perlindungan konstitusional tidak dengan sendirinya menentukan pertanggungjawaban pidana seseorang tanpa pemeriksaan terhadap unsur hukum yang berlaku (Kholil, 2026).

Perlindungan Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 1 Tahun 2024 mengubah sejumlah ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dalam kasus penyalahgunaan *deepfake*, UU ITE dapat menjadi dasar analisis apabila perbuatan dilakukan melalui sistem elektronik dan memenuhi unsur ketentuan yang relevan. Penerapan UU ITE perlu mempertimbangkan bentuk perbuatan yang dilakukan. Apabila *deepfake* digunakan untuk menyebarkan konten yang melanggar ketentuan tertentu, analisis harus diarahkan pada unsur pasal yang mengatur perbuatan tersebut. Apabila teknologi digunakan untuk memanipulasi informasi elektronik, ketentuan mengenai manipulasi informasi elektronik juga dapat dikaji sesuai unsur dan tujuan yang disyaratkan. Dengan demikian, penggunaan *deepfake* tidak otomatis memenuhi unsur tindak pidana berdasarkan UU ITE. Penegak hukum perlu membuktikan perbuatan, keterlibatan pelaku, kesalahan, dan unsur khusus yang ditentukan oleh pasal yang diterapkan.

Perlindungan Berdasarkan Undang-Undang Pelindungan Data Pribadi

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur perlindungan terhadap pemrosesan data pribadi. Dalam konteks *deepfake*, penggunaan gambar, suara, atau informasi lain yang dapat mengidentifikasi seseorang perlu dianalisis berdasarkan karakteristik data dan cara pemrosesannya. UU PDP menggolongkan data biometrik sebagai data pribadi yang bersifat spesifik. Namun, tidak setiap gambar wajah atau rekaman suara otomatis merupakan data biometrik dalam seluruh konteks. Penilaian perlu memperhatikan apakah data tersebut diproses untuk mengidentifikasi seseorang secara unik atau memenuhi karakteristik data biometrik sebagaimana dimaksud dalam peraturan. Apabila pembuatan atau penyebaran *deepfake* melibatkan pemrosesan data pribadi yang tidak sesuai dengan ketentuan hukum,

UU PDP dapat menjadi dasar untuk menilai hak subjek data dan kewajiban pihak yang memproses data tersebut. Oleh karena itu, relevansi UU PDP dalam perkara *deepfake* bergantung pada fakta mengenai sumber data, dasar pemrosesan, tujuan penggunaan, serta bentuk pelanggaran yang terjadi.

Perlindungan Berdasarkan Hukum Pidana dan Perdata

Selain UU ITE dan UU PDP, perlindungan korban dapat dikaji melalui ketentuan hukum pidana dan perdata yang relevan dengan perbuatan konkret. Apabila *deepfake* digunakan sebagai sarana untuk menipu seseorang dan memperoleh keuntungan secara melawan hukum, ketentuan mengenai penipuan dapat menjadi objek analisis. Apabila teknologi digunakan untuk membuat atau menyebarkan konten intim tanpa persetujuan, ketentuan hukum yang berkaitan dengan kekerasan seksual berbasis elektronik dan peraturan lain yang relevan perlu diperiksa. Dari perspektif perdata, korban dapat mengkaji kemungkinan gugatan berdasarkan ketentuan perbuatan melawan hukum apabila unsur-unsurnya terpenuhi. Analisis meliputi adanya perbuatan melawan hukum, kesalahan, kerugian, dan hubungan sebab akibat antara perbuatan dengan kerugian yang dialami. Dengan demikian, perlindungan hukum terhadap korban *deepfake* memerlukan pendekatan yang mempertimbangkan jenis pelanggaran dan kepentingan hukum yang terdampak.

Pertanggungjawaban Hukum terhadap Pelaku Penyalahgunaan Deepfake

Pertanggungjawaban Pidana

Pertanggungjawaban pidana terhadap pelaku penyalahgunaan *deepfake* harus didasarkan pada ketentuan hukum yang berlaku dan pembuktian unsur tindak pidana. Dalam analisis hukum pidana, perlu dibedakan antara perbuatan yang dilarang, kesalahan pelaku, dan kemungkinan adanya alasan yang menghapus pertanggungjawaban. Teknologi *deepfake* merupakan sarana yang dapat digunakan untuk melakukan berbagai jenis perbuatan, sehingga tidak tepat menetapkan satu bentuk pertanggungjawaban yang berlaku untuk semua kasus. Sebagai contoh, pihak yang membuat video palsu untuk melakukan penipuan memiliki konteks perbuatan yang berbeda dari pihak yang membuat simulasi digital untuk kepentingan film dengan persetujuan orang yang bersangkutan. Penentuan pertanggungjawaban harus memperhatikan tujuan, tindakan, keterlibatan, dan akibat yang ditimbulkan. Dengan demikian, penggunaan

teknologi AI tidak dapat menggantikan kewajiban untuk membuktikan unsur tindak pidana.

Pertanggungjawaban Perdata

Penyalahgunaan *deepfake* juga dapat menimbulkan kerugian yang menjadi dasar pengkajian pertanggungjawaban perdata. Kerugian tersebut dapat berupa kehilangan uang, kerugian reputasi, atau gangguan terhadap kehidupan pribadi. Dalam perkara perdata, korban perlu membuktikan dasar tuntutan dan unsur-unsur yang disyaratkan oleh hukum. Tidak semua kerugian yang dirasakan secara otomatis menghasilkan hak atas ganti rugi dengan jumlah tertentu. Penilaian terhadap kerugian dan pemulihannya bergantung pada bukti serta ketentuan hukum yang diterapkan. Pemulihan hak korban dapat menjadi bagian penting dalam penanganan perkara, selain penentuan sanksi terhadap pelaku.

Tanggung Jawab Platform Digital

Penyebaran konten *deepfake* dapat melibatkan pembuat konten, pengunggah, pengguna yang menyebarkan ulang, dan penyelenggara platform digital. Kedudukan dan tanggung jawab setiap pihak perlu dianalisis secara terpisah. Pembuat konten tidak selalu merupakan pihak yang mengunggahnya, sedangkan pengguna yang menyebarkan ulang dapat memiliki keterlibatan yang berbeda dari pembuat awal. Penyelenggara platform juga tidak otomatis bertanggung jawab secara pidana hanya karena konten tertentu tersedia pada layanannya. Analisis tanggung jawab platform perlu mempertimbangkan kewajiban hukum yang berlaku, mekanisme pengaduan, pengetahuan atau pemberitahuan mengenai konten, serta tindakan yang diwajibkan oleh peraturan. Pembedaan tersebut penting untuk menghindari pembebanan tanggung jawab secara berlebihan kepada pihak yang tidak terbukti melakukan atau turut serta dalam perbuatan melawan hukum.

Kendala Penegakan Hukum terhadap Penyalahgunaan *Deepfake*

Autentikasi dan Pembuktian Digital

Deepfake dapat menghasilkan konten yang menyerupai rekaman asli. Oleh karena itu, pemeriksaan secara visual atau pendengaran biasa belum tentu cukup untuk menentukan keaslian konten. Penanganan perkara dapat membutuhkan pemeriksaan forensik digital, analisis metadata, penelusuran sumber konten, serta pemeriksaan perangkat atau akun yang relevan. Hasil pemeriksaan teknis perlu dinilai bersama alat bukti lain sesuai ketentuan hukum

acara. Kendala ini menunjukkan pentingnya peningkatan kemampuan teknis dalam proses penyidikan dan pemeriksaan perkara yang melibatkan konten sintetis.

Identifikasi Pelaku

Pelaku dapat menggunakan akun anonim, identitas palsu, atau layanan digital yang berada di luar wilayah Indonesia. Kondisi tersebut dapat menyulitkan proses identifikasi dan pengumpulan bukti. Dalam perkara lintas negara, penanganan dapat memerlukan kerja sama dengan penyedia layanan atau otoritas di yurisdiksi lain. Proses tersebut harus tetap memperhatikan ketentuan hukum dan perlindungan hak individu.

Penyebaran Konten dan Pemulihan Korban

Konten *deepfake* dapat disalin dan disebarluaskan melalui berbagai platform. Penghapusan dari satu akun belum tentu menghilangkan seluruh salinan konten. Kondisi ini dapat memperpanjang kerugian yang dialami korban. Oleh karena itu, mekanisme penanganan perlu mempertimbangkan dokumentasi bukti, pelaporan kepada platform, pembatasan distribusi, dan perlindungan identitas korban. Pemulihan juga tidak cukup hanya dengan menghentikan penyebaran konten. Dalam kasus tertentu, korban mungkin membutuhkan akses terhadap bantuan hukum dan mekanisme pemulihan kerugian sesuai ketentuan yang berlaku.

Penentuan Norma Hukum yang Tepat

Karena *deepfake* dapat digunakan untuk berbagai tujuan, penentuan ketentuan hukum harus dilakukan berdasarkan perbuatan konkret. Satu kasus dapat berkaitan dengan penipuan, sedangkan kasus lain dapat berkaitan dengan pelanggaran data pribadi, pencemaran nama baik, atau penyebaran konten intim. Penerapan pasal harus mempertimbangkan unsur delik, asas legalitas, dan hubungan antara peraturan yang relevan. Kajian Fitriani dan Wahyudi (2026) membahas bahwa pengaturan tindak pidana *deepfake* dalam UU ITE dan UU PDP masih bersifat tidak langsung dan memunculkan persoalan kepastian hukum. Temuan tersebut menjadi salah satu dasar untuk menelaah kebutuhan evaluasi regulasi lebih lanjut.

Upaya Penguatan Perlindungan Hukum

Evaluasi dan Penguatan Regulasi

Penguatan regulasi perlu diarahkan pada kejelasan perlindungan korban, pembagian tanggung jawab, dan mekanisme penanganan konten sintetis yang disalahgunakan. Evaluasi perlu mengidentifikasi apakah ketentuan yang tersedia telah memadai untuk menghadapi berbagai bentuk penyalahgunaan *deepfake* atau apakah diperlukan pengaturan tambahan. Apabila pengaturan khusus dikembangkan, perumusannya perlu memperhatikan asas legalitas, kepastian hukum, perlindungan hak asasi manusia, serta keseimbangan antara pencegahan penyalahgunaan dan penggunaan teknologi yang sah.

Peningkatan Kapasitas Forensik Digital

Peningkatan kapasitas forensik digital diperlukan untuk membantu aparat penegak hukum memeriksa keaslian konten, menelusuri sumber, dan mengidentifikasi keterlibatan pihak-pihak terkait. Pelatihan dan pengembangan prosedur pemeriksaan perlu didukung oleh metode yang dapat dipertanggungjawabkan secara ilmiah. Integritas bukti elektronik juga harus dijaga agar dapat digunakan dalam proses hukum.

Penguatan Mekanisme Pengaduan

Korban perlu memperoleh akses terhadap mekanisme pengaduan yang mudah dipahami dan efektif. Mekanisme tersebut dapat mencakup pelaporan kepada platform digital, permintaan penanganan konten, serta akses kepada lembaga atau aparat yang berwenang. Proses pengaduan perlu memperhatikan kerahasiaan identitas korban dan mengurangi risiko penyebaran ulang konten yang merugikan.

Peningkatan Literasi Digital

Literasi digital berperan penting dalam mengurangi penyebaran konten sintetis yang menyesatkan. Masyarakat perlu memahami bahwa gambar, suara, dan video yang tampak autentik belum tentu merupakan rekaman peristiwa nyata. Edukasi juga perlu mencakup penghormatan terhadap privasi, persetujuan penggunaan identitas, dan tanggung jawab ketika membagikan konten digital.

Kerja Sama Antarpemangku Kepentingan

Penanganan penyalahgunaan *deepfake* memerlukan kerja sama antara pemerintah, aparat penegak hukum, penyelenggara platform, akademisi, ahli teknologi, dan masyarakat. Kerja sama tersebut dapat mendukung peningkatan kapasitas teknis, penanganan laporan, pertukaran pengetahuan, serta pengembangan kebijakan yang sesuai dengan perkembangan teknologi.

Kesimpulan

Berdasarkan hasil pembahasan, dapat disimpulkan bahwa perlindungan hukum terhadap korban penyalahgunaan *deepfake* berbasis kecerdasan buatan di Indonesia dapat dikaji melalui sejumlah instrumen hukum, antara lain UUD Negara Republik Indonesia Tahun 1945, UU ITE, UU PDP, KUHP, dan peraturan terkait. Penerapan instrumen tersebut harus didasarkan pada bentuk perbuatan, hak yang terdampak, dan terpenuhinya unsur hukum yang relevan. Pertanggungjawaban hukum terhadap pelaku dapat berupa pertanggungjawaban pidana maupun perdata sepanjang persyaratan hukum terpenuhi. Penentuan tanggung jawab perlu dilakukan secara individual dengan mempertimbangkan perbuatan, kesalahan, keterlibatan, dan bukti yang tersedia. Penggunaan teknologi *deepfake* semata tidak otomatis membuktikan adanya tindak pidana.

Penegakan hukum masih menghadapi tantangan berupa autentikasi bukti digital, identifikasi pelaku, penyebaran konten lintas platform, serta pemulihan hak korban. Oleh karena itu, diperlukan penguatan mekanisme pengaduan, peningkatan kapasitas forensik digital, koordinasi antarpemangku kepentingan, dan evaluasi regulasi untuk memberikan perlindungan hukum yang lebih efektif.

Daftar Pustaka

- Akhtar, Zahid, dkk. “*Video and Audio Deepfake Datasets and Open Issues in Deepfake Technology: Being A head of the Curve.*” *Forensic Sciences* 4 No.3 (Juli, 2024): 289-377.
- Fitriani, N. A., & Wahyudi, E. “*Kebijakan formulasi tindak pidana deepfake dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Pelindungan Data Pribadi (UU PDP) di Indonesia.*” *Jurnal Hukum to-Ra: Hukum untuk Mengatur dan Melindungi Masyarakat*, 12 No.1 (April,2026):157–169.
- Kholil, Ferdiansyah, M. “*Repositioning Digital Sovereignty as a Constitutional Right: A Critique of the Limitations of Personal Data Protection in the Era of Artificial Intelligence.*” *Qaumiyyah: Jurnal Hukum Tata Negara* 7 No. 1 (Juli, 2026): 39-57.
- Oscar Fathah, dkk. “*Reconstructing Legal Protection for Deepfake Victims in Indonesia.*” *Jurnal Ilmu Hukum Keadilan*, 8 No.1 (Juli, 2026): 746-766.
- Republik Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

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

Republik Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Republik Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Seveny, Madalaine Christella, dkk. "Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi." *Disiplin: Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda*, 31 No.2 (April,2025): 97-106.

Widyanto, M. A., Waldo, R., & Ramadan, T. A. "Reconstructing legal protection for victims of deepfake abuse through a victim-oriented justice approach." *Jurnal Kepastian Hukum dan Keadilan*, 8, No.1 (Juni, 2026): 287-300

Wirasmara, A. P. "Perlindungan hukum terhadap korban penyalahgunaan deepfake berbasis artificial intelligence (AI) di Indonesia." *Jurnal Riset Multidisiplin Edukasi*, 3, No.6 (Juni, 2026): 915–924.



Syariah: Jurnal Hukum Keluarga Islam

is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).