

Urgensi Pengaturan Hukum terhadap *Deepfake* sebagai Alat Kejahatan Siber dalam Perspektif KUHP dan UU ITE

¹Dimas Kresna Prayoga, ²Ibrahim Fikma Edrisy

^{1,2}Universitas Terbuka, Indonesia

¹dimaskresna642@gmail.com

ABSTRACT

The advancement of digital technology has given rise to the phenomenon of deepfakes – artificial intelligence (AI)-based technology that enables realistic manipulation of audio, video, or images. Although deepfakes hold positive potential, they have also emerged as new tools in cybercrime, including fraud, non-consensual pornography, and defamation. This article aims to analyze the urgency of legal regulation regarding deepfakes in the context of the Indonesian Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE). The research method employed is normative juridical, using statutory and case study approaches. The findings indicate that current legal regulations do not explicitly address the use of deepfake technology, thus necessitating regulatory updates to provide more effective legal protection. This article recommends the establishment of specific legal provisions in national legislation to mitigate the negative impacts of deepfake misuse.

Keywords: *Deepfake, Cybercrime, KUHP, UU ITE, Technology Regulation*

ABSTRAK

Perkembangan teknologi digital telah melahirkan fenomena *deepfake*, yaitu teknologi berbasis kecerdasan buatan (AI) yang memungkinkan manipulasi audio, video, atau gambar secara realistis. Meskipun memiliki potensi positif, *deepfake* juga menjadi alat baru dalam kejahatan siber seperti penipuan, pornografi non-konsensual, dan pencemaran nama baik. Artikel ini bertujuan untuk menganalisis urgensi pengaturan hukum terhadap *deepfake* dalam konteks KUHP dan UU ITE. Metode penelitian yang digunakan adalah normatif yuridis dengan pendekatan perundang-undangan dan studi kasus. Hasil kajian menunjukkan bahwa pengaturan hukum yang ada belum secara eksplisit mengatur penggunaan teknologi *deepfake*, sehingga diperlukan pembaruan regulasi untuk memberikan perlindungan hukum yang lebih efektif. Artikel ini merekomendasikan adanya pengaturan khusus dalam perundang-undangan nasional guna menanggulangi dampak negatif dari penyalahgunaan teknologi *deepfake*.

Kata kunci: *Deepfake, Kejahatan Siber, KUHP, UU ITE, Regulasi Teknologi.*

Pendahuluan

Perkembangan digital teknologi pada era sekarang terlebih yang berfokus pada sosial media telah membawa dampak yang sangat besar dalam segala aspek kehidupan, terlebih di bidang komunikasi dan informasi berbasis sosial media. Salah satu dampak perubahan yang menjadi perhatian utama dalam dunia secara keseluruhan adalah fitur *deepfake*, yaitu fitur yang berbasis kecerdasan buatan (*artificial intelligence/AI*) yang bisa merubah atau memanipulasi konten video dengan sangat realistis sehingga sulit untuk dibedakan mana yang asli dan mana yang palsu tanpa bantuan program tertentu. Meski fenomena *deepfake* ini bisa membawa perubahan yang positif dari sisi seperti bidang perfilman, edukasi atau hiburan, fenomena ini juga dapat membawa potensi negatif yang luar biasa besar jika digunakan oleh pihak yang salah terutama jika berfokus di bidang kejahatan siber. Publikasi atau penyebaran video secara audio dan visual yang menyerupai

tokoh terkenal dibidang *entertainment* atau olahraga serta *public figure* terkenal dapat memberikan dampak negatif ditengah masyarakat seperti manipulasi identitas atau pencemaran nama baik yang bisa saja berdampak gangguan pada stabilitas sosial dan keamanan terhadap data pribadi seseorang atau kelompok.

Di Indonesia, hukum yang diatur telah berlaku dalam memberikan sanksi atau tindakan tegas kepada pelaku di bidang kejahatan siber yang berdasarkan pada Kitab Undang-Undang Hukum Pidana (KUHP) serta diatur pula pada Undang-Undang Nomor 11 Tahun 2008 yang berfokus pada Informasi dan Transaksi Elektronik (UU ITE) beserta beberapa perubahannya. Namun, jika ditinjau lebih jauh dasar hukum tersebut belum relevan untuk menjangkau fenomena *deepfake* secara khusus dan spesifik karena fenomena *deepfake* ini masih tergolong fenomena baru di bidang teknologi baru. Ketiadaan peraturan dan dasar hukum yang jelas dalam fenomena ini telah memunculkan banyak pertanyaan serta kebingungan tentang efektivitas kekuatan hukum yang sudah ada dalam mencegah serta merespond efek negatif dalam penyalahgunaan *deepfake*. Berdasarkan pertimbangan tersebut, penulis membuat kajian yang lebih mendalam tentang urgensi pengaturan hukum terhadap fenomena *deepfake* dalam perspektif KUHP dan UU ITE yang pada dasarnya telah dianggap menjadi penting untuk segera dilaksanakan, hal ini juga berguna untuk menjamin kepastian hukum serta dapat menjadi instrument dasar perlindungan bagi masyarakat di era kemajuan digital saat ini.

Berdasarkan latar belakang permasalahan serta fenomena tersebut, tulisan ini akan berfokus untuk membahas tiga rumusan masalah yang menjadi pokok utamanya. Pertama, bagaimana bentuk penyalahgunaan teknologi *deepfake* sebagai alat kejahatan siber? Kedua, bagaimana ketentuan dalam KUHP serta UU ITE dalam mengatur serta mengantisipasi penyalahgunaan *deepfake*? Ketiga, apa urgensi pengaturan hukum yang lebih berfokus atau spesifik yang mengatur tentang fenomena teknologi *deepfake* di Indonesia? Penulis berharap agar kajian ini bisa memberikan dampak positif serta kontribusi pemikiran nyata dalam usaha serta upaya pembaruan hukum pidana nasional supaya lebih responsif terhadap majunya era perkembangan teknologi informasi yang sekarang dirasa bersifat sangat dinamis.

Metode Penelitian

Penelitian ini menggunakan metode yuridis normatif, yaitu pendekatan yang menitikberatkan pada studi kepustakaan dan analisis peraturan perundang-undangan. Penulis menggunakan pendekatan konseptual, pendekatan perundang-undangan, serta pendekatan kasus untuk menganalisis efektivitas dan kekosongan hukum terkait *deepfake*.

Hasil Penelitian dan Pembahasan

Bentuk Penyalahgunaan Teknologi *Deepfake* sebagai Alat Kejahatan Siber

Pengertian singkat & karakter bahaya

Deepfake adalah teknik sintesis media (video, gambar, audio) berbasis kecerdasan buatan yang mampu menghasilkan representasi visual/sonik seseorang yang tampak otentik padahal palsu. Karakteristiknya: (i) meniru wajah/suara nyata; (ii) sulit dibedakan dengan mata/telinga biasa; (iii) dapat diproduksi dan disebarkan cepat melalui platform digital. Karena itu *deepfake* berpotensi menjadi sarana untuk berbagai kejahatan: pencemaran nama baik, pemerasan/penipuan, pornografi non-konsensual, propaganda, manipulasi politik, sampai sabotase reputasi institusi. Bentuk-bentuk penyalahgunaan yang umum ditemukan:

- a) *Deepfake* pornografi (*non-consensual sexual imagery*) – memanipulasi wajah korban ke tubuh aktor pornografi; sering dipakai untuk memeras, merusak reputasi, atau

menakut-nakuti korban. Kasus-kasus serupa sudah banyak muncul dan digolongkan sebagai pelanggaran pornografi sekaligus pelanggaran hak pribadi. (Hukum & Hukum, 2025)

- b) Pencemaran nama baik dan fitnah – video/audio palsu dibuat untuk menuduhkan tindakan tercela terhadap seseorang (misal menyatakan korupsi, pernyataan bermuatan fitnah) sehingga merugikan kehormatan. Penyebaran ke publik mengakibatkan kerugian reputasi dan materiil. (1, 2, 3, 2025)
- c) Penipuan dan pemerasan – pelaku menggunakan *deepfake* untuk menipu pihak ketiga (misal otorisasi transaksi, panggilan suara CEO palsu – *CEO fraud*) atau memeras korban dengan ancaman menyebarkan materi palsu. (Priya et al., 2025)
- d) Disinformasi dan manipulasi politik – manipulasi pidato tokoh publik menjelang pemilu atau peristiwa publik untuk mengacaukan opini publik atau merusak legitimasi. (Nurdin et al., 2025)

Dampak hukum dan non-hukum

Dampak *deepfake* bersifat multi-dimensi: kerugian personal (trauma, kehilangan pekerjaan), sosial (polarisasi, ketidakpercayaan publik), ekonomi (penipuan finansial), dan keamanan nasional (manipulasi informasi). Secara hukum, masalah utama muncul pada: klasifikasi tindak pidana yang tepat; pembuktian/forensik bukti digital; keterkaitan subjek hukum (pembuat, penyebar, platform); dan simultanitas norma (KUHP, UU ITE, UU PDP, UU Pornografi, serta aturan platform).

Bagaimana KUHP dan UU ITE Mengatur atau Mengantisipasi Penyalahgunaan *Deepfake*

Kerangka normatif yang relevan (dasar hukum utama) Di Indonesia saat ini tidak ada satu norma yang secara eksplisit menyebut istilah *deepfake*. Namun terdapat beberapa norma pidana dan regulasi yang dapat dimanfaatkan untuk menjerat penyalahgunaan *deepfake*:

- a. UU ITE (Undang-Undang Nomor 11 Tahun 2008 dan perubahan-perubahannya; Perubahan terakhir tercatat dalam UU No. 1 Tahun 2024/2023 yang merevisi ketentuan tertentu) – mengatur tindak pidana bidang informasi elektronik, termasuk pasal-pasal terkait pornografi, pencemaran nama baik/serangan kehormatan melalui informasi elektronik, manipulasi informasi, dan pembuatan/penyebaran konten yang melanggar kesusilaan. Misalnya, pasal yang mengatur muatan kesusilaan, pasal yang mengatur pencemaran nama baik berbasis elektronik (Pasal 27A/Pasal terkait dalam redaksi terbaru) serta Pasal 35 tentang manipulasi Informasi Elektronik. Pemanfaatan ketentuan-ketentuan ini untuk *deepfake* telah menjadi rujukan praktik penuntutan dan kajian akademik. (1, 2, 3, 2025)
KUHP (Kitab Undang-Undang Hukum Pidana) – Pasal tentang penghinaan pencemaran nama baik (Pasal 310-311 KUHP), pemalsuan (jika *deepfake* digunakan untuk memalsukan bukti), dan ketentuan baru pada KUHP baru/penyesuaian yang memasukkan ketentuan terkait pornografi dan kejahatan siber (beberapa literatur menunjukkan KUHP baru memuat pasal-pasal relevan). KUHP dapat digunakan untuk menjerat pelaku *deepfake* yang unsur tindak pidana klasiknya terpenuhi (misal fitnah, penipuan, atau pemalsuan). (Rencang et al., 2025)
- b. UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) – mengatur pemrosesan data pribadi, kewajiban pengendali data, dan sanksi bagi pemrosesan data pribadi yang melanggar. Pembuatan *deepfake* yang memanfaatkan data pribadi (foto, suara) dapat diproses sebagai pelanggaran terhadap UU PDP, khususnya jika diproduksi tanpa persetujuan subjek data atau dengan maksud merugikan. UU PDP juga mengatur hak subjek data untuk menghapus/dilakukan koreksi. (Wanda & Putri,

2025)

- c. UU Pornografi & KUHP baru – *Deepfake* bermuatan pornografi dapat dikenai ketentuan pornografi (mis. Pasal 27 UU ITE redaksi baru, Pasal 407 KUHP baru), selain ketentuan UU ITE/UU PDP. Studi menunjukkan penegakan terhadap *deepfake porn* telah diproses memakai kombinasi norma ini. (Novera & Z, 2024)

Penerapan norma terhadap kasus *deepfake* – kekuatan dan keterbatasan Kekuatan:

- a) Adanya UU ITE dan UU PDP memberi pangkalan normatif: penyebaran konten elektronik yang memuat fitnah atau pornografi dapat dikenai sanksi, begitu pula pengolahan data pribadi tanpa izin. Hal ini berarti pelaku *deepfake* dapat dijerat melalui pasal-pasal tersebut apabila unsur-unsurnya terpenuhi. Contoh praktik penuntutan telah menerapkan pasal UU ITE untuk kasus pornografi *deepfake* dan pencemaran nama baik. (Arvitto, 2025)

Keterbatasan & tantangan praktik:

- a) Ketiadaan definisi khusus: Karena undang-undang tidak secara eksplisit mendefinisikan –*synthetic media/deepfake*, aparat penegak harus menafsirkan ketentuan umum (misalnya manipulasi informasi, pemalsuan, pencemaran nama baik) untuk menangani kasus ini. Hal ini berisiko menimbulkan ketidakpastian hukum dan variasi putusan. Beberapa studi menyatakan bahwa kekosongan definisi menghambat klasifikasi tindak pidana dan pembuktian. (Khusna & Pangestuti, 2019)
- b) Pembuktian forensik digital: *Deepfake* sering dirancang untuk mengelabui proses forensik misalnya menghilangkan metadata, menambahkan noise sehingga membuktikan unsur kesengajaan pembuat dan keterkaitan tindakan dengan pelaku memerlukan kemampuan teknis tinggi dan pengetahuan forensik multimedia. Dokumen ilmiah menyoroti tantangan pembuktian bukti digital *deepfake* dalam persidangan. (Pengguna et al., 2024)
- c) *Mens rea* (unsur kesengajaan) dan niat jahat: Untuk beberapa tindak pidana (mis. pencemaran nama baik), harus dibuktikan bahwa terdakwa sengaja menyerang kehormatan. Ketika seseorang membagikan *deepfake* yang dibuat pihak lain, pembuktian unsur sengaja, pengetahuan bahwa konten itu palsu, dan maksud mempublikasikan menjadi isu kompleks. UU ITE terbaru mencoba memperbaiki redaksi untuk menangani penyebaran bermuatan kehormatan, namun praktiknya masih menuntut interpretasi. (Karunia et al., 2025)
- d) Peran platform dan yurisdiksi: Penyebaran platform lintas negara menimbulkan masalah yurisdiksi dan kerjasama penyitaan data. Regulasi platform (*take down obligation*) dan kerja sama internasional diperlukan namun masih menjadi kendala. Literatur kebijakan merekomendasikan mekanisme *notice and takedown* serta kerangka kerjasama regional/internasional. (Kadir et al., 2025)

Ringkasan posisi hukum saat ini

Secara prinsip, KUHP, UU ITE dan UU PDP menyediakan instrumen untuk menjerat pelaku *deepfake* dalam berbagai macam tindak pidana (pencemaran nama baik, pornografi, penipuan, pemalsuan) dan pelanggaran privasi. Namun, karena tidak ada aturan yang secara spesifik mendefinisikan dan mengatur *deepfake/synthetic media*, penegakan memerlukan interpretasi lintas norma, menimbulkan ketidakpastian hukum, dan menuntut kapasitas teknis aparat penegak.

Urgensi Pengaturan Hukum yang Lebih Spesifik terhadap Teknologi *Deepfake* di Indonesia

Alasan urgensi (argumentasi hukum-normatif dan praktis)

- e) Kepastian hukum: Prinsip kepastian hukum (*legal certainty*) menghendaki bahwa

perbuatan yang dapat menimbulkan sanksi pidana harus jelas terbatas dan dapat dipahami. Tanpa definisi dan ketentuan khusus, aparat dan pengadilan menyederhanakan kasus *deepfake* lewat norma-norma umum yang berisiko inkonsistensi putusan. Ketiadaan definisi "*deepfake*" bertentangan dengan *asas lex certa*. Studi akademik menunjukkan kebutuhan definisi agar pembedaan antara kritik, parodi, dan kriminalitas menjadi lebih jelas. (Rencang et al., 2025)

- f) Kekhususan modus operandi: *Deepfake* bukan sekadar penyebaran konten; ia menciptakan bukti palsu yang bisa menjerat korban dalam perkara pidana/perdata, memanipulasi bukti elektronik, dan mengelabui proses verifikasi. Oleh karena itu diperlukan ketentuan khusus yang menyoar produksi, distribusi, dan penggunaan *deepfake* untuk tujuan kriminal (misal pasal baru yang menyoar pembuatan dan distribusi konten sintesis yang meniru identitas tanpa izin). (Ekosistemnya & Sumatera, 2025)
- g) Perlindungan hak fundamental: *Deepfake* menyentuh hak atas nama baik, kehormatan, privasi, dan perlindungan data pribadi. UU PDP sudah menjawab sebagian, namun perlu sinkronisasi antara UU PDP, UU ITE, dan KUHP dengan aturan khusus yang mengatur larangan produksi/penyebaran *deepfake* tanpa persetujuan serta hak pemulihan korban (*remedy & takedown*). Putusan-putusan Mahkamah Konstitusi terkait perlindungan data dan UU PDP juga menguatkan keniscayaan perlindungan lebih spesifik. (Wanda & Putri, 2025)
- h) Kebutuhan mekanisme respons cepat: Karena *deepfake* menyebar sangat cepat, dibutuhkan mekanisme respons cepat—kewajiban platform untuk *take-down*; prosedur verifikasi cepat; serta sanksi administratif yang dapat segera dijatuhkan sebelum kerusakan reputasi meluas. Tanpa aturan khusus, proses hukum pidana yang panjang tidak efektif mengatasi dampak awal. Kajian kebijakan merekomendasikan kombinasi sanksi administratif dan pidana serta mekanisme perintah penghapusan cepat. (Juli, 2025)
- i) Kesiapan forensik dan kapasitas penegakan: Negara wajib membangun kapasitas forensik multimedia, melatih penegak hukum, dan mengatur standar pembuktian bukti sintesis. Peraturan khusus bisa mengamankan pembentukan laboratorium forensik khusus dan *standard operating procedure* (SOP) pembuktian *deepfake*. Literatur menunjukkan kesulitan pembuktian sebagai salah satu kendala utama penuntutan. (Journal, 2025)

Rekomendasi norma dan arsitektur regulasi yang perlu dipertimbangkan

Berdasarkan analisis hukum komparatif dan kajian akademik, berikut usulan norma konkret yang mendesak:

- a) Definisi hukum —*synthetic media*∥/*deepfake*: Undang-undang (atau peraturan pelaksana) harus memasukkan definisi operasional (misal —Informasi elektronik berbentuk audio, gambar, atau video yang dihasilkan atau dimodifikasi menggunakan teknik pembelajaran mesin atau algoritma lainnya sehingga meniru citra/ucapan seseorang secara realistis tanpa persetujuan subjek∥). Definisi ini mesti menyoar elemen teknik dan konteks penggunaan. (mengatasi kekaburan terminologis). (Dalam & Pornografi, 2025)
- b) Kewajiban persetujuan & larangan produksi/distribusi tanpa izin: Aturan tegas yang melarang pembuatan atau menyebarkan *deepfake* yang meniru identitas seseorang tanpa persetujuan jika tujuan merugikan, bersifat pornografi, atau menimbulkan fitnah. Sanksi berjenjang: administratif (denda, pemblokiran), perdata (ganti rugi, *injunctive relief*), pidana untuk kasus berat (pemerasan, penipuan, pornografi). UU PDP dapat

menangani pemrosesan data pribadi; ketentuan baru akan mensinergikan keduanya. (No Title, 2024)

- c) Kewajiban platform (*intermediary liability & take-down*): Mengatur kewajiban operator platform untuk cepat menanggapi *notice-and-takedown* atas konten *deepfake*, menyimpan *log provenance*, dan bekerja sama dengan pihak berwenang; atur batas waktu respons; dan sanksi jika platform lalai (kecuali untuk *content moderation* yang wajar). Hal ini diperlukan karena peredaran cepat *deepfake*. (Ai & Transaksi, 2025)
- d) Standar pembuktian forensik & kewajiban pelaporan: Menetapkan standar forensik digital untuk identifikasi *deepfake*, pembentukan laboratorium nasional, serta kewajiban melaporkan insiden tertentu ke otoritas (misal ketika *deepfake* menyerang tokoh publik atau menimbulkan ancaman keamanan). Regulasi teknis ini memfasilitasi proses penuntutan. (Nomor, 2025)
- e) Perlindungan hak korban dan remediasi cepat: Atur hak korban untuk mendapatkan perintah penghapusan cepat (*court/administrative takedown*), hak pemulihan reputasi, serta mekanisme ganti rugi. Ini memastikan pemulihan lebih cepat daripada proses pidana panjang. (Rohmawati et al., 2024)
- f) Pembedaan antara tujuan kriminal dan *legitimate uses*: Regulasi harus melindungi penggunaan sah (seni, penelitian, parodi) dengan mempertimbangkan faktor konteks, niat, dan transparansi (misal kewajiban label *—synthetic!* jika bukan untuk menipu). Pengaturan ini menjaga keseimbangan antara kebebasan berekspresi dan pencegahan kriminalitas. (Sy, 2025)
- g) Koordinasi lintas-regulasi: Pengaturan *deepfake* harus sinkron antara UU ITE (konten & transaksi elektronik), UU PDP (data pribadi), UU Pornografi (muatan pornografi), serta KUHP (tindak pidana umum). Pemerintah perlu menerbitkan pedoman teknis terpadu dan membangun satu unit respons nasional (seperti CSIRT khusus *deepfake*). (Islam et al., 2024)

Argumen kebijakan

- a) *Preemptive effect*: Regulasi khusus menimbulkan efek pencegahan dan meningkatkan kesadaran publik; lebih efektif mencegah penyebaran awal *deepfake*.
- b) Kepastian penegakan: Memudahkan aparat dalam menetapkan pasal yang relevan dan mempercepat putusan; mengurangi ketergantungan pada penafsiran beragam terhadap norma lama.
- c) Harmonisasi teknologi & hukum: Menyediakan kerangka kerja yang responsif terhadap perkembangan teknologi dan menuntut penyesuaian teknis (forensik, standar deteksi).
- d) Perlindungan hak asasi: Menjaga reputasi, privasi, dan hak politik warga negara dari serangan berbasis teknologi canggih.

Penutup

Deepfake adalah tantangan baru dalam dunia kejahatan siber. Hingga saat ini, Indonesia masih memerlukan instrumen hukum yang jelas sebagai bentuk antisipasi serta responsif untuk mengatasi fenomena *deepfake*. Hal ini dirasa sangat perlu karena hingga kini belum ada dasar hukum yang mengatur kejahatan siber khususnya dalam fenomena kasus penyalahgunaan *deepfake* secara eksplisit. Teknologi ini telah digunakan dalam berbagai bentuk kejahatan yang merugikan individu dan masyarakat secara luas. KUHP dan UU ITE hanya dapat digunakan secara terbatas karena belum mampu mencakup secara menyeluruh kompleksitas dan risiko teknologi *deepfake*. Sehingga untuk mengurangi dampak negatif yang terlalu besar serta permasalahan yang kompleks diperlukan instrument hukum yang jelas untuk mencegah serta menyelesaikan permasalahan

fenomena penyalahgunaan *deepfake* secara eksplisit.

Daftar Pustaka

- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas UU ITE.
- Kitab Undang-Undang Hukum Pidana (KUHP).
- Hadjon, P. M. (1987). *Perlindungan Hukum bagi Rakyat di Indonesia*. Surabaya: Bina Ilmu.
- Achmad, Y. (2023). *Cybercrime dan Perkembangan Teknologi Digital*. Jakarta: Prenada Media.
- Sari, N. (2022). "Deepfake sebagai Ancaman Privasi dan Urgensi Pengaturannya". *Jurnal Hukum & Teknologi*, 5(1), 45–60.
- Simanjuntak, D. (2021). *Hukum Siber di Indonesia*. Yogyakarta: FH UGM Press.
- Effendi, A. (2020). "Kejahatan Siber dan Tantangan Penegakan Hukum di Era Digital". *Jurnal Ilmu Hukum*, 14(2), 101–119.
- OECD (2022). *Deepfake Technology and the Law*. OECD Digital Policy Report. 1, 2, 3. (2025). 01. Ai, P., & Transaksi, D. (2025). *PLATFORM DIGITAL*. 06(01), 44–53.
- Arvitto, R. S. (2025). *Implikasi Hukum Deepfake : Telaah terhadap UU ITE dan UU PDP (Legal Implications of Deepfake : A Review of the ITE Law and the PDP Law)*. 4(2), 73– 82.
- Dalam, D., & Pornografi, K. (2025). *Perlindungan hukum bagi korban penggunaan deepfake dalam kejahatan pornografi*. 2(1).
- Ekosistemnya, D. A. N., & Sumatera, D. I. (2025). *No Title*.
- Hukum, F., & Hukum, J. (2025). *Penyalahgunaan Teknologi Deepfake untuk Konten Pornografi Non- Konesual di Indonesia*. April.
- Islam, U., Muhammad, K., & Banjarmasin, A. A. (2024). *Rewang Rencang : Jurnal Hukum Lex Generalis*. Vol. 5. No.7 (2024) Tema/Edisi : Hukum Pidana (Bulan Ketujuh) <https://jhlg.rewangrencang.com/>. 5(7), 1–15.
- Journal, M. L. A. W. (2025). *Maleo law journal*. 9(2).
- Juli, V. N. (2025). *Urgensi Reformasi Hukum Pidana Indonesia dalam Menjerat Pelaku Deepfake Pornografi Berbasis Artificial intelligence pornografi telah menjadi masalah yang cukup mengkhawatirkan di kalangan Penegakan hukum terhadap penyalahgunaan AI dalam kasus kendala , terutama karena regulasi yang ada seperti Undang-Undang ITE ,. 12–26.*
- Kadir, Z. K., Hukum, F., & Muslim, U. (2025). *Kejahatan Berbasis Identitas Digital : Menggagas Kebijakan Kriminal untuk Dunia Metaverse*. 12(2022), 124–137.
- Karunia, M., Maan, P., Amalo, H., & Dede, N. (2025). *Analisis Perlindungan Hukum terhadap Penyimpangan Artificial Intelligence dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana perundang-undangan dan pendekatan konseptual , proses analisa yang meliputi metode , menganalisis regulasi penyimpangan artificial intelligence (AI) dalam tindak pidana deepfake masalah penyimpangan artificial intelligence (AI) dalam tindak pidana deepfake pornografi . Primer , Bahan Hukum Sekunder , dan Bahan Hukum Tersier . Peneliti akan mencari peraturan. 296– 307.*
- Khusna, I. H., & Pangestuti, S. (2019). *Deepfake , Tantangan Baru Untuk Netizen Deepfake, a New Challenge for Netizen*. 2, 1–24.
- No Title*. (2024). 1, 44–45.
- Nomor, V. (2025). *Jurnal Media Hukum*. 13(September), 207–219.
- Novera, O., & Z, Y. F. (2024). *Analisis Pengaturan Hukum Pidana terhadap Penyalahgunaan Teknologi Manipulasi Gambar (Deepfake) dalam Penyebaran Konten Pornografi Melalui Akun Media Sosial*. 10(2), 460–474.

- Nurdin, S. W., Nugraha, I. F., Hasanuddin, U., Article, I., Security, N., & Commons, C. (2025). *ANCAMAN DEEPFAKE DAN DISINFORMASI BERBASIS AI : IMPLIKASI TERHADAP KEAMANAN SIBER DAN STABILITAS*. 4(01), 73–92.
- Pengguna, P., Deepfake, T., Pidana, T., Nama, P., & Berbasis, B. (2024). *Jurnal pacta sunt servanda*. 5(September), 120–129.
- Priya, D., Pane, R., & Tambe, A. W. (2025). *Tantangan Penegakan Hukum dan Upaya Mitigasi atas Hadirnya Deepfake Porn sebagai Jenis Tindak Pidana Digital pada Era Artificial Intelligence*. 1.
- Rencang, R., Hukum, J., Generalis, L., Pidana, H., & Ketujuh, B. (2025). *Rewang Rencang : Jurnal Hukum Lex Generalis*. Vol.6. No.7 (2025) Tema/Edisi : Hukum Pidana (Bulan Ketujuh) <https://jhlg.rewangrencang.com/>. 6(7), 1–13.
- Rohmawati, I., Junaidi, A., & Khaerudin, A. (2024). *Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO)*. 4, 1779–1794.
- Sy, M. F. (2025). *DEEPFAKE PORNOGRAFI : STUDI KONSTITUSI DAN PENEGAKANNYA DI INDONESIA*. 8(2), 113–128.
- Wanda, D., & Putri, S. (2025). *Perlindungan hak privasi dalam penyalahgunaan teknologi*. 14, 195–210.