

**PERTANGGUNGJAWABAN PIDANA ATAS DEEPPFAKE AI DALAM
PRODUKSI DAN DISTRIBUSI PORNOGRAFI DIGITAL DI INDONESIA**
*CRIMINAL LIABILITY FOR AI DEEPPFAKE IN THE PRODUCTION AND
DISTRIBUTION OF DIGITAL PORNOGRAPHY IN INDONESIA*

Kevin David Sirait, Arman Saut Rivando, Cecilia Angel, Zico Ricardo

Aritonang dan Lenny Maria Aritonang

Criminal Law and Green Economy, Universitas Prima Indonesia

Korespondensi Penulis : kevinliposirait@gmail.com

Citation Structure Recommendation :

Sirait, Kevin David, Arman Saut Rivando, Cecilia Angel, Zico Ricardo Aritonang dan Lenny Maria Aritonang. *Pertanggungjawaban Pidana atas Deepfake AI dalam Produksi dan Distribusi Pornografi Digital di Indonesia*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.7. No.7 (2026).

ABSTRAK

Perkembangan teknologi deepfake berbasis Artificial Intelligence melahirkan kejahatan pornografi digital manipulatif yang kompleks. Penelitian ini menganalisis pengaturan hukum dan pertanggungjawaban pidana di Indonesia. Hasilnya, regulasi seperti Undang-Undang Pornografi dan Undang-Undang ITE belum secara spesifik mengatur deepfake, menimbulkan kekosongan hukum (legal vacuum). Meskipun demikian, pelaku dapat dijerat secara interpretatif melalui ketentuan yang ada. Dari aspek pertanggungjawaban pidana, pelaku yang memproduksi dan mendistribusikan konten deepfake pornografi dapat dimintai pertanggungjawaban apabila memenuhi unsur actus reus dan mens rea. Namun, terdapat kendala dalam pembuktian dan identifikasi pelaku akibat anonimitas serta sifat lintas batas teknologi digital.

Kata Kunci: Artificial Intelligence, Deepfake, Pertanggungjawaban Pidana, Pornografi Digital

ABSTRACT

The development of deepfake technology based on Artificial Intelligence has given rise to complex manipulative digital pornography crimes. This study analyzes the legal framework and criminal liability in Indonesia. The results show that regulations such as the Pornography Law and the ITE Law have not specifically regulated deepfake, creating a legal vacuum. Nevertheless, perpetrators can be prosecuted interpretatively through existing provisions. Regarding criminal liability, perpetrators who produce and distribute deepfake pornographic content can be held accountable if the elements of actus reus and mens rea are fulfilled. However, there are obstacles in evidence and perpetrator identification due to anonymity and the borderless nature of digital technology.

Keywords: Artificial Intelligence, Criminal Liability, Deepfake, Digital Pornography

A. PENDAHULUAN

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*—selanjutnya disebut AI) dalam satu dekade terakhir telah melahirkan transformasi besar dalam ekosistem digital global, termasuk munculnya teknologi *deepfake* yang memungkinkan manipulasi identitas seseorang secara visual maupun auditori dengan tingkat realisme yang sulit dibedakan dari kenyataan.¹ Teknologi *deepfake* yang dibangun menggunakan metode *Generative Adversarial Network* (GAN) ini pada awalnya dikembangkan untuk kepentingan inovatif dalam industri hiburan dan produksi film,² namun seiring dengan semakin luasnya akses publik terhadap perangkat lunak berbasis AI, teknologi ini mulai disalahgunakan untuk berbagai tujuan yang melanggar hukum, termasuk produksi dan distribusi konten pornografi digital tanpa persetujuan korban (*non-consensual deepfake pornography*).³ Secara filosofis, penyalahgunaan teknologi *deepfake* dalam pornografi digital menimbulkan persoalan mendasar mengenai martabat manusia, hak atas privasi dan integritas identitas digital sebagai bagian dari hak asasi manusia yang harus dilindungi oleh negara. Pemerintah Indonesia sendiri telah menyatakan bahwa praktik *deepfake* seksual tanpa persetujuan merupakan pelanggaran serius terhadap hak asasi manusia, martabat individu, serta rasa aman publik di ruang digital.⁴

Secara yuridis, Indonesia sebenarnya telah memiliki sejumlah instrumen hukum yang dapat digunakan untuk menindak kejahatan pornografi digital, antara lain Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi (Undang-Undang Pornografi, 2008), Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) (Undang-Undang ITE, 2016), serta Kitab Undang-Undang Hukum Pidana (KUHP) Nasional yang mulai berlaku pada 2 Januari 2026.

¹ Robert Chesney dan Danielle Citron, *Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics*, Foreign Affairs, Vol.98, No.1 (2019).

² Ian J. Goodfellow, dkk., *Generative Adversarial Nets*, Prosiding Advances in Neural Information Processing Systems (2014).

³ Jan H. Kietzmann, dkk., *Deepfakes: Trick or Treat?*, Business Horizons, Vol.63, No.2 (2020).

⁴ Friska Yolandha, *Komdigi Putus Akses Sementara Grok, Lindungi Warga dari Pornografi AI*, diakses dari <https://ameera.republika.co.id/berita/t8msv2370/komdigi-putus-akses-sementara-grok-lindungi-warga-dari-pornografi-ai?>, diakses pada 29 April 2026.

KUHP Nasional melalui Pasal 172 dan Pasal 407 secara tegas mengatur ancaman pidana bagi pihak yang memproduksi, membuat, memperbanyak, menggandakan, menyebarkan, serta menyiarkan konten pornografi dengan ancaman pidana penjara paling singkat 6 bulan dan paling lama 10 tahun atau pidana denda.⁵ Namun demikian, pengaturan yang ada saat ini masih bersifat umum dan belum secara spesifik mengatur konten digital hasil manipulasi berbasis kecerdasan buatan seperti *deepfake*. Ketiadaan regulasi khusus yang secara eksplisit mengatur produksi dan distribusi konten pornografi berbasis AI ini menimbulkan kekosongan hukum (*legal vacuum*) serta ketidakpastian dalam penegakan hukum,⁶ terutama dalam hal pembuktian unsur kesalahan (*mens rea*) dan identifikasi pelaku yang sering kali menggunakan identitas anonim atau beroperasi lintas batas negara.⁷

Secara sosiologis, fenomena pornografi digital berbasis *deepfake* telah menjadi ancaman nyata di tengah masyarakat, terutama bagi perempuan yang menjadi target utama kejahatan ini. Berdasarkan laporan global, dalam kurun waktu 2019 hingga 2023 jumlah video *deepfake* di internet meningkat sebesar 550%, dengan 98% di antaranya merupakan konten pornografi dan 99% korbannya adalah perempuan. Di Indonesia sendiri, kasus-kasus penyalahgunaan teknologi *deepfake* untuk pornografi digital semakin marak, termasuk kasus mahasiswa Universitas Udayana yang memproduksi konten *deepfake* terhadap puluhan mahasiswi serta kasus penipuan yang mencatut nama Gubernur Khofifah Indar Parawansa melalui manipulasi video *deepfake*. Kementerian Komunikasi dan Digital (Komdigi) bahkan telah mengambil langkah tegas dengan memblokir sementara layanan Grok AI milik X (sebelumnya Twitter) karena digunakan untuk memproduksi dan mendistribusikan konten asusila tanpa persetujuan pemiliknya. Realitas sosiologis ini menunjukkan bahwa kejahatan *deepfake* pornografi bukan sekadar persoalan kesusilaan, melainkan telah menjadi bentuk

⁵ Indonesia, *Undang-Undang tentang Kitab Undang-Undang Hukum Pidana*, UU No.1 Tahun 2023, LN Tahun 2023 No.1, TLN No.6842.

⁶ Gefy Caesarati Zumarno, Sri Jaya Lesmana dan Ratna Indayatun, *Bridging Legal Gaps in AI-Generated Deepfake Pornography: A Comparative Approach to Privacy and Digital Ethics*, Jurnal Ius Constituendum, Vol.11, No.2 (2026).

⁷ Nurulhuda Irawati, Ismansyah dan Nani Mulyati, *Pertanggungjawaban Pidana Deepfake Porn Berbasis AI: Studi Perbandingan dan Implikasi Global*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.7, No.1 (2026), p.1-28.

kekerasan berbasis teknologi yang berpotensi menimbulkan kerugian psikologis, sosial, hingga reputasional yang masif dan berkelanjutan bagi korban.⁸

Berbagai penelitian terdahulu telah mengkaji fenomena penyalahgunaan teknologi *deepfake* dari berbagai perspektif. Penelitian oleh⁹ menemukan bahwa instrumen hukum Indonesia saat ini, termasuk UU ITE, UU Pornografi dan UU Perlindungan Data Pribadi, belum secara eksplisit mengatur *deepfake* pornografi, sehingga mengakibatkan ketidakpastian hukum, tantangan penegakan hukum, serta perlindungan korban yang tidak memadai. Penelitian oleh¹⁰ dalam studi perbandingan dengan Australia dan Korea Selatan menunjukkan bahwa sementara Indonesia masih menggunakan aturan lama yang berfokus pada pornografi umum, Australia telah memiliki *The Criminal Code Amendment (Deepfake Sexual Material) Act 2024*¹¹ dan Korea Selatan telah menerapkan ketentuan yang lebih luas dalam *The Act on Special Cases Concerning the Punishment of Sexual Crimes*¹². Penelitian oleh¹³ mengidentifikasi bahwa perlindungan hukum terhadap penyalahgunaan *deepfake* saat ini masih terbatas dan sangat bergantung pada interpretasi UU ITE dan KUHP. Penelitian oleh¹⁴ merekomendasikan reformulasi hukum yang lebih adaptif terhadap perkembangan teknologi AI serta penguatan strategi pembuktian yang relevan dengan karakteristik bukti digital. Penelitian oleh¹⁵ dalam perspektif viktimologi menegaskan bahwa perlindungan hukum yang ada saat ini belum mampu memberikan keadilan dan pemulihan yang memadai bagi korban, sehingga diperlukan pendekatan yang berorientasi pada pemulihan korban (*victim recovery and rehabilitation*).

⁸ Loso Judijanto, Andrew Shandy Utama dan Heri Setiyawan, *Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia*, The Easta Journal Law and Human Rights, Vol.3, No.2 (2025).

⁹ Gefy Caesarati Zumarno, Sri Jaya Lesmana dan Ratna Indayatun, *Op.Cit.*.

¹⁰ Nurulhuda Irawati, Ismansyah dan Nani Mulyati, *Op.Cit.*.

¹¹ Parliament of Australia, *Criminal Code Amendment (Deepfake Sexual Material) Act 2024*, No. 78, 2024, Federal Register of Legislation.

¹² South Korea, *Act on Special Cases Concerning the Punishment of Sexual Crimes*, Pub. L. No. 17264 (2020).

¹³ Rizky Karo Karo, Zein Jiddan dan Hanan Atanto Buono, *Analisis dalam Kasus Penyalahgunaan Deepfake dari Segi Perlindungan Data Pribadi dalam UU ITE dan UU PDP di Indonesia*, Prosiding Seminar Nasional Pendidikan, Ilmu-Ilmu Sosial dan Hukum, Vol.1, No.1 (2026).

¹⁴ Yolanda Frisky Amelia, Arfan Kaimuddin dan Hisbul Luthfi Ashsyarofi, *Pertanggungjawaban Pidana Pelaku terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake menurut Hukum Positif Indonesia*, Dinamika, Vol.30, No.1 (2024).

¹⁵ Adnasohn Aqilla Respati, dkk., *Analisis Hukum terhadap Pencegahan Kasus Deepfake serta Perlindungan Hukum terhadap Korban*, Media Hukum Indonesia, Vol.2, No.2 (2024).

Berdasarkan uraian di atas, dapat dipahami bahwa penyalahgunaan teknologi *deepfake* berbasis AI dalam produksi dan distribusi pornografi digital merupakan fenomena yang menimbulkan berbagai persoalan hukum yang kompleks, baik dari aspek filosofis, yuridis, maupun sosiologis. Perkembangan teknologi kecerdasan buatan telah membuka peluang bagi munculnya bentuk-bentuk kejahatan baru yang menantang sistem hukum pidana tradisional¹⁶, sementara regulasi yang ada di Indonesia belum sepenuhnya mampu mengakomodasi karakteristik kejahatan digital yang bersifat manipulatif, sintetis, non-konsensual, lintas batas, serta sulit dilacak¹⁷. Oleh karena itu, penelitian mengenai pertanggungjawaban pidana terhadap penyalahgunaan teknologi *deepfake* berbasis Artificial Intelligence dalam produksi dan distribusi pornografi digital menjadi penting untuk dilakukan. Adapun rumusan masalah dalam penelitian ini adalah sebagai berikut: (1) Bagaimana pengaturan hukum terhadap penyalahgunaan teknologi *deepfake* berbasis AI dalam pornografi digital di Indonesia? (2) Bagaimana pertanggungjawaban pidana pelaku yang memproduksi dan mendistribusikan konten pornografi berbasis *deepfake*?

B. PEMBAHASAN

1. Pengaturan Hukum terhadap Penyalahgunaan Teknologi *Deepfake* Berbasis AI dalam Pornografi Digital di Indonesia

a. Konsep dan Perkembangan Teknologi *Deepfake*

Teknologi *deepfake* berbasis Artificial Intelligence menggunakan metode Deep Learning dan Generative Adversarial Network (GAN) untuk menghasilkan konten visual atau audio yang sangat realistis. Awalnya dikembangkan untuk industri hiburan, namun kini banyak disalahgunakan untuk produksi pornografi tanpa persetujuan korban. Perkembangan ini menimbulkan tantangan hukum karena konten *deepfake* sulit dibedakan dari aslinya.¹⁸

¹⁶ Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, Praeger, Santa Barbara, 2010.

¹⁷ Mireille Hildebrandt, *Law for Computer Scientists and Other Folk*, Oxford University Press, Oxford, 2020.

¹⁸ Ian J. Goodfellow, dkk., *Op.Cit.*.

Tabel 1. Perbandingan Aspek Teknologi Deepfake

ASPEK	TAHAP AWAL	PEKEMBANGAN SAAT INI
Pengguna	Profesional (industri film)	Masyarakat umum
Teknologi	Terbatas, mahal	Mudah diakses, open-source
Tujuan Resiko	Hiburan & efek visual Relatif rendah	Hiburan, edukasi, hingga kejahatan Tinggi (penipuan, pornografi, disinformasi)

Tabel ini membandingkan empat aspek teknologi *deepfake* antara tahap awal dan perkembangan saat ini. Pada tahap awal, pengguna terbatas pada profesional industri film dengan teknologi yang mahal dan terbatas, tujuan utamanya untuk hiburan dan efek visual, serta risiko relatif rendah. Saat ini, masyarakat umum dapat mengakses teknologi open-source dengan mudah, tujuan bervariasi dari hiburan hingga kejahatan dan risiko yang ditimbulkan sangat tinggi, termasuk penipuan, pornografi dan disinformasi.

b. Karakteristik Pornografi Digital Berbasis AI

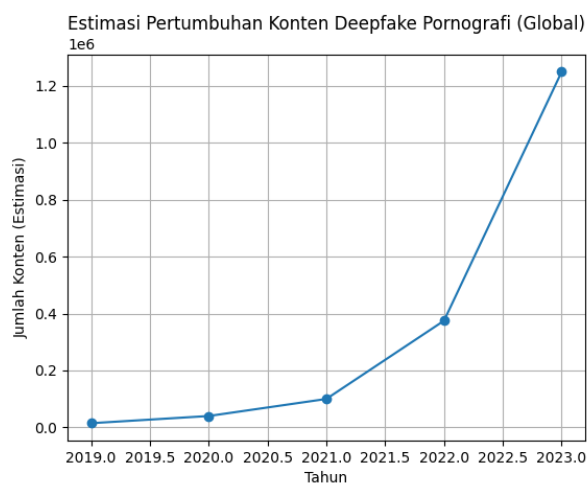
Pornografi digital berbasis AI memiliki karakteristik yang membedakannya dari pornografi konvensional. Pertama, konten dihasilkan tanpa keterlibatan nyata subjek (non-konsensual). Kedua, biaya produksi rendah dan proses cepat. Ketiga, distribusi masif dan instan melalui platform digital. Keempat, pelaku dapat beroperasi secara anonim dan lintas batas negara. Kelima, dampak psikologis dan sosial terhadap korban bersifat permanen karena jejak digital sulit dihapus.¹⁹

Tabel 2. Perbandingan Karakteristik

ASPEK	PORNOGRAFI KONVENSIONAL	PORNOGRAFI BERBASIS AI
Keterlibatan Subjek	Nyata (aktor terlibat langsung)	Tidak nyata (rekayasa digital)
Teknologi	Kamera & produksi manual	AI & deep learning
Biaya Produksi	Relatif tinggi	Relatif rendah
Kecepatan Produksi	Lama	Sangat cepat
Distribusi	Terbatas	Global & instan
Risiko Penyalahgunaan	Moderat	Sangat tinggi

¹⁹ Mary Anne Franks, *Sexual Harassment 2.0*, Maryland Law Review, Vol.71, No.3 (2012).

Tabel ini membandingkan enam aspek antara pornografi konvensional dan pornografi berbasis AI. Pada pornografi konvensional, subjek terlibat secara nyata, menggunakan teknologi kamera manual, biaya produksi relatif tinggi, waktu produksi lama, distribusi terbatas dan risiko penyalahgunaan moderat. Sebaliknya, pornografi berbasis AI tidak melibatkan subjek nyata, menggunakan teknologi AI dan deep learning, biaya rendah, produksi sangat cepat, distribusi global dan instan, serta risiko penyalahgunaan sangat tinggi.



Gambar 1. Grafik Peningkatan Konten *Deepfake* Pornografi Global

Grafik tersebut menunjukkan kecenderungan peningkatan eksponensial, yang menandakan bahwa tanpa intervensi regulasi dan teknologi yang memadai, fenomena ini akan terus berkembang secara signifikan. Dengan demikian, karakteristik pornografi digital berbasis AI yang meliputi sifat realistis tanpa persetujuan, kemudahan produksi, distribusi masif, anonimitas, serta lintas yurisdiksi menunjukkan tingkat kompleksitas yang jauh lebih tinggi dibandingkan pornografi konvensional. Kondisi ini menuntut adanya pendekatan hukum yang tidak hanya represif, tetapi juga preventif dan adaptif terhadap perkembangan teknologi. Dalam konteks hukum pidana Indonesia, hal ini menjadi tantangan besar, terutama dalam merumuskan norma yang mampu menjangkau bentuk-bentuk kejahatan baru berbasis teknologi digital.

c. Regulasi Pornografi dalam Hukum Indonesia

Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi mendefinisikan pornografi secara luas, namun belum secara eksplisit mengatur konten hasil rekayasa digital berbasis AI. Kitab Undang-Undang Hukum Pidana (KUHP) Nasional (UU No. 1 Tahun 2023) Pasal 172 dan 407 mengatur ancaman pidana bagi produksi dan distribusi pornografi, tetapi juga tidak menyebut *deepfake*. Ketiadaan pengaturan mengenai persetujuan (consent) dalam representasi digital menjadi celah hukum utama.²⁰

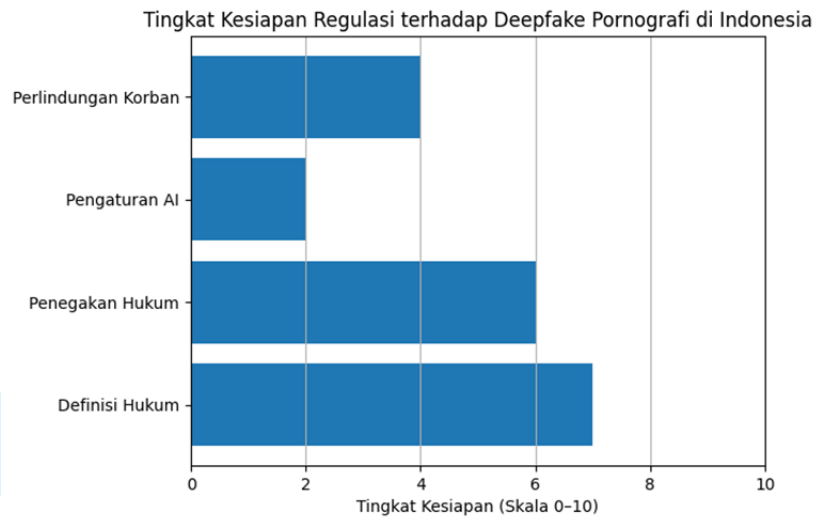
Tabel 3. Analisis normatif UU Pornografi, KUHP dan tantangan pada *deepfake*

Aspek	UU Pornografi (2008)	KUHP (Lama & Baru)	Tantangan pada <i>Deepfake</i>
Fokus Pengaturan	Materi pornografi	Perbuatan melanggar kesusilaan	Tidak spesifik
Subjek Hukum	Individu & korporasi	Individu	Tidak mengatur identitas digital
Media	Konvensional & digital umum	Konvensional	Tidak eksplisit pada AI
Unsur Persetujuan	Tidak diatur rinci	Terbatas	Krusial dalam <i>deepfake</i>
Teknologi AI	Tidak diatur	Tidak diatur	Menjadi celah hukum

Tabel ini menganalisis lima aspek pengaturan. UU Pornografi berfokus pada materi pornografi dengan subjek individu dan korporasi, mencakup media konvensional dan digital umum, tetapi tidak mengatur unsur persetujuan secara rinci dan tidak menyentuh teknologi AI. KUHP (lama dan baru) berfokus pada perbuatan melanggar kesusilaan dengan subjek individu, media konvensional dan juga tidak mengatur teknologi AI. Tantangan pada *deepfake* adalah tidak spesifiknya regulasi yang ada,

²⁰ Gefy Caesarati Zumarno, Sri Jaya Lesmana dan Ratna Indayatun, *Op.Cit.*.

tidak diaturnya identitas digital, tidak eksplisitnya media AI, serta pentingnya unsur persetujuan yang menjadi krusial.



Gambar 2. Tingkat Kesiapan Regulasi terhadap *Deepfake* Pornografi di Indonesia

Diagram tersebut menunjukkan bahwa kelemahan utama terletak pada aspek pengaturan teknologi dan perlindungan korban, yang belum berkembang seiring dengan pesatnya inovasi digital. Dalam perspektif hukum pidana modern, kondisi ini mencerminkan adanya legal gap atau kekosongan hukum. Hukum positif Indonesia masih berorientasi pada pendekatan konvensional, sementara kejahatan telah berkembang ke arah digital berbasis algoritma. Oleh karena itu, diperlukan reformulasi kebijakan hukum yang mampu mengakomodasi perkembangan teknologi, baik melalui revisi undang-undang yang ada maupun pembentukan regulasi baru yang secara khusus mengatur kejahatan berbasis AI. Dengan demikian, meskipun Indonesia telah memiliki instrumen hukum untuk mengatur pornografi, efektivitasnya dalam menghadapi pornografi digital berbasis AI masih terbatas. Hal ini menegaskan urgensi pembaruan hukum pidana yang tidak hanya bersifat represif, tetapi juga adaptif terhadap dinamika teknologi serta berorientasi pada perlindungan hak korban

d. Pengaturan Konten Digital dalam UU ITE

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) Pasal 27 ayat (1) melarang distribusi, transmisi, atau pembuatan dapat diaksesnya informasi elektronik yang melanggar kesusilaan. Ketentuan ini dapat menjerat pelaku distribusi *deepfake* pornografi. Namun UU ITE lebih berfokus pada distribusi, bukan produksi konten. Selain itu, pembuktian menghadapi tantangan karena alat bukti elektronik dan pelaku sering anonim.²¹

Tabel 4. Aspek UU ITE

Aspek	UU ITE
Fokus Pengaturan	Distribusi & akses konten digital
Dasar Hukum	Pasal 27 ayat (1)
Cakupan Teknologi	Umum (tidak spesifik AI)
Kelebihan	Adaptif terhadap media elektronik
Kelemahan	Tidak mengatur produksi <i>deepfake</i>

Tabel ini merangkum posisi UU ITE. Fokus pengaturannya adalah distribusi dan akses konten digital. Dasar hukum utama adalah Pasal 27 ayat (1). Cakupan teknologi bersifat umum dan tidak spesifik AI. Kelebihan UU ITE adalah adaptif terhadap media elektronik secara umum. Kelemahannya adalah tidak mengatur produksi *deepfake* secara khusus, sehingga fase produksi konten manipulatif tidak terjangkau.

e. Analisis Kecukupan Regulasi terhadap *Deepfake*

Regulasi yang ada di Indonesia belum sepenuhnya memadai untuk mengatasi kejahatan *deepfake* pornografi. Ketiadaan pengaturan eksplisit tentang produksi konten *deepfake* menimbulkan kekosongan hukum (legal vacuum). Penegak hukum harus melakukan interpretasi ekstensif yang berpotensi melanggar asas legalitas. Perlindungan korban masih bersifat parsial. Indonesia saat ini masih bersifat reaktif, belum proaktif dalam mengantisipasi perkembangan teknologi AI.²²

Penelitian oleh Azis (2025) misalnya, secara tegas memaparkan bahwa hukum positif Indonesia masih mengandung kekosongan norma,

²¹ Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press, Amsterdam, 2011.

²² Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*, Prenada Media Group, Jakarta, 2016.

baik dalam aspek sanksi yang berorientasi pada pidana penjara, keterbatasan pemulihan korban digital, maupun ketiadaan mekanisme pengendalian teknologi AI secara preventif, khususnya pada pengaturan dalam Undang-Undang ITE.²³ Ketidadaan pengaturan eksplisit tentang produksi konten deepfake ini menjadi celah hukum utama.

Akibatnya, penegak hukum harus melakukan interpretasi ekstensif terhadap undang-undang yang ada. Namun, pendekatan interpretatif ini berpotensi melanggar asas legalitas (*nullum delictum, nulla poena sine praevia lege poenali*). Lebih lanjut, Hifni et al. (2025) dalam studinya tentang tindak pidana pornografi di ruang digital menemukan adanya tumpang tindih pengaturan antara Undang-Undang Pornografi dan Undang-Undang ITE.²⁴ Penelitian tersebut menyimpulkan bahwa dari perspektif asas *Lex Specialis Legi Generali*, penerapan Undang-Undang ITE seharusnya lebih relevan karena mengatur secara khusus perbuatan melalui media elektronik, namun pilihan dakwaan yang hanya berfokus pada Undang-Undang Pornografi berpotensi menimbulkan ketidakpastian hukum dan menyebabkan perlindungan terhadap korban menjadi kurang optimal.

Selain itu, penelitian oleh Ghazmi (2021) yang membahas tentang pengaturan AI di Indonesia juga relevan untuk memperkuat temuan ini.²⁵ Hasil penelitiannya menunjukkan bahwa belum diakuinya AI sebagai subjek hukum di Indonesia, baik secara perdata maupun pidana, dapat menimbulkan berbagai masalah hukum. Studi ini merekomendasikan pembentukan regulasi spesifik yang mengatur AI sebagai langkah preventif, serta penerapan doktrin vicarious liability untuk meminta pertanggungjawaban atas tindakan AI kepada orang atau badan hukum yang mengendalikannya.

²³ Abdul Azis, *Rekonstruksi Hukum Penyalahgunaan Artificial Intelligence (AI) dalam Konten Kesusilaan dan Pencemaran Nama Baik*, Rewang Rencang : Jurnal Hukum Lex Generalis, Vol.6, No.7 (2025).

²⁴ Mohammad Hifni, Safiulloh dan Mutiara Rizka Azzahra, *Tindak Pidana Pornografi dalam Putusan Pengadilan Negeri Sleman Nomor 220/Pid.Sus/2022/PN Sleman*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.6, No.7 (2025).

²⁵ Shabrina Fadiah Ghazmi, *Urgensi Pengaturan Artificial Intelligence pada Sektor Bisnis Daring di Indonesia*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.2, No.8 (2021).

Dengan demikian, Indonesia saat ini masih bersifat reaktif, belum proaktif dalam mengantisipasi perkembangan teknologi AI. Tanpa pembaruan hukum yang mendasar, kekosongan hukum ini akan terus dimanfaatkan oleh pelaku kejahatan siber dan perlindungan hukum terhadap korban tetap tidak optimal.

f. Kelemahan Pengaturan Hukum yang Ada

Terdapat enam kelemahan utama pengaturan hukum di Indonesia terhadap kejahatan deepfake pornografi, yang jika dibandingkan dengan perkembangan di negara seperti Amerika Serikat, semakin mempertegas adanya kekosongan hukum (*legal vacuum*).

Pertama, ketiadaan regulasi khusus. Indonesia masih mengandalkan interpretasi atas undang-undang yang ada. Sebaliknya, Amerika Serikat telah memiliki *TAKE IT DOWN Act* yang ditandatangani pada 19 Mei 2025, yang secara tegas mengkriminalisasi publikasi gambar intim non-konsensual, termasuk yang dihasilkan oleh AI/deepfake.²⁶

Kedua, ambiguitas rumusan delik. Sebagai perbandingan, negara bagian *North Carolina* telah merevisi statuta mereka sehingga definisi "gambar" mencakup "representasi atau gambaran visual digital atau buatan komputer yang dibuat, diadaptasi, atau dimodifikasi melalui sarana teknologi, seperti algoritma atau kecerdasan buatan".²⁷

Ketiga, kesulitan pembuktian. Aikey (2026) menegaskan bahwa gugatan hukum tradisional seringkali tidak sesuai untuk menangani sifat kejahatan deepfake yang unik, karena sulitnya mengonfirmasi otentisitas dan asal-usul konten digital.²⁸ Di AS, pendekatan dengan "standar orang yang berakal sehat" (*reasonable person test*) telah diadopsi untuk mengatasi tantangan ini.

²⁶ Taylor Greeno, *Take It Down or Take it Too Far? The Legal Fallout of New Online Takedown Powers*, North Carolina Journal of Law & Technology, Vol.27, No.2 (2025).

²⁷ J. Royce Fichtner dan Troy J. Strader, *Criminalizing Deepfakes: A Comprehensive Review of US Legislative Responses to Synthetic Media Abuse*, Journal of the Midwest Association for Information Systems, Vol.1, No.3 (2026).

²⁸ Kennedy Aikey, *Fabricated Images, Real Harm: The DEFIANCE Act and Federal Civil Remedies for Deepfake Pornography*, University of Cincinnati Law Review Blog, Vol.94 (2026).

Keempat, lemahnya akuntabilitas platform. Di AS, *TAKE IT DOWN Act* mewajibkan platform online untuk menghapus konten dalam waktu 48 jam setelah menerima pemberitahuan yang sah, dengan pengawasan penegakan hukum oleh Federal Trade Commission (FTC). Kegagalan mematuhi kewajiban ini dapat mengakibatkan tindakan hukum.²⁹

Kelima, ketidaksinkronan antarregulasi. Sebagai perbandingan, selain *TAKE IT DOWN Act* (pendekatan pidana), Kongres AS juga mengupayakan *DEFIANCE Act* yang menciptakan hak gugat perdata bagi korban untuk menuntut ganti rugi terhadap pembuat digital forgeries.³⁰ Keberadaan kedua kerangka hukum yang saling melengkapi ini menawarkan perlindungan yang lebih komprehensif.

Keenam, lemahnya perlindungan korban dan mekanisme penghapusan konten. Fichtner dan Strader (2026) mengidentifikasi bahwa meskipun terjadi ekspansi legislatif yang pesat, masih terdapat variasi signifikan dalam definisi dan cakupan undang-undang antarnegara bagian.³¹ Namun, *TAKE IT DOWN Act* telah menetapkan standar federal untuk penghapusan konten dalam 48 jam.³² Sebaliknya, Indonesia saat ini belum memiliki mekanisme hukum yang sekomprehensif ini.

g. Konsep Ideal Pengaturan *Deepfake* di Masa Depan

Untuk mengatasi legal vacuum dan berbagai kelemahan regulasi yang telah diuraikan sebelumnya, diperlukan suatu konsep pengaturan *deepfake* yang ideal dan adaptif terhadap perkembangan teknologi. Kerangka hukum yang ideal tidak cukup hanya bersifat reaktif, tetapi harus proaktif dalam merespons kemajuan kecerdasan buatan.³³ Setidaknya terdapat tiga pilar utama dalam konsep ideal ini.

Pertama, perlunya kriminalisasi eksplisit dan reformulasi tindak pidana. Penelitian oleh Meliana (2025) secara tegas mengemukakan urgensi pembentukan formulasi pidana khusus untuk *deepfake* dalam

²⁹ Taylor Greeno, *Op.Cit.*.

³⁰ Kennedy Aikey, *Op.Cit.*.

³¹ J. Royce Fichtner dan Troy J. Strader, *Op.Cit.*.

³² Taylor Greeno, *Op.Cit.*.

³³ Abdul Azis, *Op.Cit.*.

sistem hukum pidana nasional, karena kerangka hukum saat ini belum mampu menjangkau kompleksitas kejahatan *deepfake*.³⁴ Azis (2025) juga menemukan adanya kekosongan norma (*normative gap*) dalam hukum positif Indonesia terkait penyalahgunaan AI dalam konten kesusilaan.³⁵ Kedua peneliti ini sepakat bahwa diperlukan reformulasi hukum yang adaptif dengan pendekatan keadilan restoratif, baik melalui pengesahan undang-undang khusus AI maupun revisi UU ITE untuk memasukkan pasal yang secara eksplisit melarang produksi, distribusi dan kepemilikan konten *deepfake* pornografi non-konsensual.

Kedua, penguatan konsep model pertanggungjawaban berlapis (*layered accountability*). Putri, Nurmasitha dan Neisyia (2025) dalam analisis pertanggungjawaban terhadap penyalahgunaan teknologi *deepfake* menekankan bahwa kekosongan hukum spesifik dan tantangan identifikasi pelaku lintas batas memerlukan pembagian tanggung jawab yang jelas.³⁶ Model ini membagi tanggung jawab kepada tiga pihak utama: (1) pengembang AI yang dapat dikenakan prinsip kehati-hatian terkait desain dan keamanan produk; (2) operator platform yang bertanggung jawab atas konten *deepfake* yang beredar di layanannya berdasarkan prinsip kelalaian; dan (3) pengguna akhir yang bertanggung jawab langsung sebagai pelaku utama. Pendekatan ini lebih komprehensif karena menjangkau seluruh rantai produksi dan distribusi *deepfake*.

Ketiga, harmonisasi regulasi dan kewajiban pelabelan konten. Azis (2025) merekomendasikan rekonstruksi hukum yang adaptif dan berkeadilan, termasuk harmonisasi antara KUHP Nasional, UU ITE, UU Pornografi, UU Perlindungan Data Pribadi dan aturan khusus AI di masa depan. Selain itu, Chalil dan Fathurrahim (2026) di dalam kajiannya tentang perlindungan martabat dan privasi perempuan menemukan bahwa kerangka hukum yang ada masih parsial dan belum efektif,

³⁴ Yang Meliana, *Urgensi Formulasi Perlindungan Hukum dan Kepastian Pidana terhadap Pengaturan Tindak Pidana Deepfake dalam Sistem Hukum Pidana Nasional*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.6, No.7 (2025).

³⁵ Abdul Azis, *Op.Cit.*.

³⁶ Nabilatul Alimah Putri, Nabilah Nurmasitha dan Ni Luh Neisyia, *Analisis Pertanggungjawaban Perdata terhadap Penyalahgunaan Teknologi Artificial Intelligence (Deepfake)*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.6, No.12 (2025).

sehingga diperlukan rekonstruksi perlindungan hukum berbasis hak asasi manusia, keadilan gender, serta etika digital.³⁷ Kedua penelitian ini memperkuat pentingnya harmonisasi regulasi dan penerapan kewajiban pelabelan konten sintetis yang jelas (*mandatory synthetic content labeling*) untuk melindungi konsumen informasi di ruang digital.

Lebih jauh, konsep ideal ini harus mengatur aspek perlindungan hukum yang lebih komprehensif bagi korban. Meliana (2025) menegaskan bahwa kriminalisasi harus mencakup produksi, penyebaran, hingga kepemilikan konten *deepfake* pornografi non-konsensual, serta didukung mekanisme penghapusan konten cepat (*takedown*), pelestarian bukti digital, restitusi yang memadai dan kerja sama lintas negara (*mutual legal assistance*).³⁸ Chalil dan Fathurrahim (2026) juga menyoroti bahwa *deepfake* pornografi merupakan pelanggaran serius terhadap martabat dan privasi perempuan, sehingga perlindungan korban harus berorientasi pada pemulihan hak-hak korban dan penguatan etika digital.³⁹ Pendekatan ini sejalan dengan urgensi untuk memastikan bahwa perlindungan hukum benar-benar berpihak pada korban.

Dengan merangkum ketiga pilar di atas, dapat disimpulkan bahwa pembentukan regulasi yang adaptif dan komprehensif bukan lagi sekadar opsi, melainkan sebuah keniscayaan untuk menciptakan kepastian hukum, menutup kekosongan norma dan memperkuat perlindungan publik terhadap kejahatan berbasis kecerdasan buatan di Indonesia.

2. Pertanggungjawaban Pidana Pelaku yang Memproduksi dan Mendistribusikan Konten Pornografi Berbasis *Deepfake*

a. Konsep Pertanggungjawaban Pidana dalam Hukum Pidana

Pertanggungjawaban pidana didasarkan pada *asas geen straf zonder schuld* (tidak ada pidana tanpa kesalahan). Menurut Moeljatno (2008), unsur-unsurnya meliputi: (1) perbuatan melawan hukum (*actus reus*), (2) kesalahan (*mens rea*) dan (3) kemampuan bertanggung jawab.

³⁷ Nurhayati Chalil dan Fathurrahim, *Perlindungan Hukum atas Martabat dan Privasi Perempuan dari Praktik Deepfake Pornografi*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.6, No.12 (2025).

³⁸ Yang Meliana, *Op.Cit.*.

³⁹ Nurhayati Chalil dan Fathurrahim, *Op.Cit.*.

Dalam kejahatan digital, teknologi AI tetap sebagai alat, bukan subjek hukum. Manusia yang mengoperasikannya bertanggung jawab. Dalam kasus *deepfake*, *actus reus* berupa produksi dan distribusi konten pornografi manipulatif; *mens rea* berupa kesengajaan yang dibuktikan dari niat dan pengetahuan pelaku.⁴⁰

Tabel 5. Hubungan antara unsur-unsur pertanggungjawaban pidana

Unsur	Penjelasan	Relevansi pada <i>Deepfake</i>
Perbuatan (<i>Actus Reus</i>)	Tindakan yang melanggar hukum	Produksi/penyebaran konten <i>deepfake</i>
Kesalahan (<i>Mens Rea</i>)	Sikap batin pelaku	Niat memanipulasi atau merugikan
Kemampuan Bertanggung Jawab	Kondisi psikis pelaku	Pelaku sadar dan memahami teknologi

Tabel ini menjelaskan tiga unsur pertanggungjawaban pidana dan relevansinya pada kasus *deepfake*. Unsur perbuatan (*actus reus*) berarti adanya tindakan melanggar hukum, yang dalam *deepfake* berupa produksi dan penyebaran konten. Unsur kesalahan (*mens rea*) berarti sikap batin pelaku, yang dalam *deepfake* berupa niat memanipulasi atau merugikan korban. Unsur kemampuan bertanggung jawab berarti kondisi psikis pelaku, yang dalam *deepfake* mengandaikan pelaku sadar dan memahami teknologi yang digunakannya.⁴¹

b. Unsur-Unsur Tindak Pidana Pornografi Digital

Tindak pidana pornografi digital memiliki unsur objektif dan subjektif. Unsur objektif mencakup perbuatan nyata seperti memproduksi, memperbanyak, menyimpan, mentransmisikan, atau menyebarluaskan konten pornografi. Dalam *deepfake*, manipulasi wajah tanpa persetujuan memenuhi unsur ini. Unsur subjektif mencakup kesengajaan (*dolus*) atau kelalaian (*culpa*). Dalam *deepfake* pornografi,

⁴⁰ Susan W. Brenner, *Op.Cit.*.

⁴¹ Juandry Aruan, *Legal Protection for Victims of Photo Abuse through Artificial Intelligence Technology in Pornography Crimes in Indonesia*, Law & Society Review, Vol.5, No.2 (2025).

kesengajaan lebih dominan karena pelaku secara sadar dan terencana menggunakan teknologi AI.⁴²

Tabel 6. Kategorisasi Perbuatan

Jenis Perbuatan	Bentuk dalam Pornografi Digital	Relevansi <i>Deepfake</i>
Produksi	Membuat konten pornografi	Manipulasi wajah/video
Reproduksi	Menggandakan konten	Edit ulang atau remix
Distribusi	Menyebarkan melalui internet	Upload ke platform digital
Aksesibilitas	Membuat dapat diakses publik	Sharing link/hosting

Tabel ini mengkategorikan empat jenis perbuatan dalam pornografi digital. Produksi (membuat konten pornografi) relevan dengan *deepfake* sebagai manipulasi wajah/video. Reproduksi (menggandakan konten) relevan sebagai edit ulang atau remix. Distribusi (menyebarkan melalui internet) relevan sebagai upload ke platform digital. Aksesibilitas (membuat dapat diakses publik) relevan sebagai sharing link atau hosting.

Tabel 7. Perbedaan Jenis Kesalahan

Jenis Kesalahan	Karakteristik	Contoh dalam <i>Deepfake</i>
Kesengajaan (Dolus)	Ada niat & kehendak	Sengaja membuat video pornografi palsu
Kelalaian (Culpa)	Kurang hati-hati	Tidak sengaja menyebarkan konten tanpa verifikasi

Tabel ini membedakan dua jenis kesalahan. Kesengajaan (dolus) memiliki karakteristik adanya niat dan kehendak, contoh dalam *deepfake* adalah sengaja membuat video pornografi palsu. Kelalaian (culpa) memiliki karakteristik kurang hati-hati, contoh dalam *deepfake* adalah tidak sengaja menyebarkan konten tanpa verifikasi.

c. Analisis Unsur Kesalahan Pelaku *Deepfake*

Kesalahan dalam kasus *deepfake* berbentuk kesengajaan (dolus), bahkan dolus eventualis (pelaku sadar risiko tapi tetap melanjutkan).

⁴² Aris Munandar AR, dkk., *Peran Niat (Mens Rea) dalam Pertanggungjawaban Pidana di Indonesia*, JIMMI: Jurnal Ilmiah Mahasiswa Multidisiplin, Vol.1, No.3 (2024).

Indikator kesengajaan meliputi: adanya perencanaan (pengumpulan data korban), penggunaan perangkat lunak AI secara sadar dan tujuan merugikan korban (misalnya memperlakukan, balas dendam, atau keuntungan ekonomi). Pembuktian mens rea sulit karena anonimitas pelaku dan sifat semi-otomatis AI, sehingga diperlukan forensik digital (analisis metadata, jejak digital, riwayat penggunaan perangkat lunak).⁴³

Tabel 8. Analisis Bentuk Kesalahan dan Indikator

Bentuk Kesalahan	Karakteristik	Indikator dalam <i>Deepfake</i>
Dolus (Kesengajaan)	Ada niat & kehendak	Merencanakan, membuat dan menyebarkan konten
Culpa (Kelalaian)	Kurang hati-hati	Lalai menyebarkan tanpa verifikasi
Dolus Eventualis	Menyadari risiko	Tahu dampak tapi tetap melanjutkan

Tabel ini merinci tiga bentuk kesalahan. Dolus (kesengajaan) dengan indikator merencanakan, membuat dan menyebarkan konten. Culpa (kelalaian) dengan indikator lalai menyebarkan tanpa verifikasi. Dolus eventualis dengan indikator tahu dampak tetapi tetap melanjutkan. Dalam *deepfake*, bentuk yang paling sering muncul adalah dolus dan dolus eventualis.⁴⁴

d. Subjek yang Dapat Dimintai Pertanggungjawaban Pidana

Terdapat tiga subjek utama yang dapat dimintai pertanggungjawaban pidana dalam kasus *deepfake* pornografi. Pertama, pembuat konten (creator) sebagai pelaku utama (dader) yang secara aktif memproduksi konten *deepfake* menggunakan perangkat lunak AI. Dasar hukum: Pasal 4 ayat (1) jo. Pasal 29 UU Pornografi. Kedua, pengunggah (uploader) yang mengunggah konten ke platform digital, dapat dikenakan Pasal 27 ayat (1) jo. Pasal 45 ayat (1) UU ITE. Ketiga, distributor atau penyebar (distributor) yang memperluas distribusi melalui reshare atau tautan, dapat dikualifikasikan sebagai turut serta (*medepleger*) atau pembantu (*medeplichtige*) (Moeljatno, 2008; Ashworth, 2013).

⁴³ Eoghan Casey, *Op.Cit.*.

⁴⁴ Muhammad Faturrachman Sy, *Deepfake Pornografi: Studi Konstitusi dan Penegakannya di Indonesia*, Legislatif, Vol.8, No.2 (2025).

e. Analisis Penerapan Pertanggungjawaban Pidana dalam Kasus Deepfake Pornografi

Penerapan pertanggungjawaban pidana di Indonesia saat ini menggunakan pendekatan interpretatif terhadap norma yang ada. Pembuat konten dikenakan pasal "memproduksi" pornografi, sedangkan pengunggah dan penyebar dikenakan pasal "mendistribusikan" konten melanggar kesusilaan. Namun penerapan ini menghadapi kendala: (1) pembuktian mens rea sulit karena pelaku anonim; (2) kualifikasi perbuatan pidana masih diperdebatkan; (3) disparitas putusan berpotensi terjadi; (4) belum ada yurisprudensi yang memadai. Diperlukan pembaruan hukum yang spesifik mengenai *deepfake*, penguatan kapasitas aparat dalam forensik digital, serta peningkatan kerja sama lintas negara.⁴⁵

Tabel 9. Penerapan pertanggungjawaban Pidana

Tahap Perbuatan	Subjek	Dasar Hukum	Bentuk Pertanggungjawaban
Produksi	Pembuat	UU Pornografi	Pelaku utama (<i>dader</i>)
Publikasi	Pengunggah	UU ITE	Pelaku langsung
Distribusi	Penyebar	UU ITE	Turut serta (<i>medepleger</i>)

Tabel ini merinci penerapan berdasarkan tahap perbuatan. Tahap produksi dengan subjek pembuat, dasar hukum UU Pornografi, bentuk pertanggungjawaban sebagai pelaku utama. Tahap publikasi dengan subjek pengunggah, dasar hukum UU ITE, bentuk pertanggungjawaban sebagai pelaku langsung. Tahap distribusi dengan subjek penyebar, dasar hukum UU ITE, bentuk pertanggungjawaban sebagai turut serta. Dengan demikian, pertanggungjawaban pidana dalam kasus *deepfake* bersifat berlapis (*multi-layered liability*).

⁴⁵ Tesalonika Liony Polandos, Wenly R. J. Lolong dan Merry Lenda Kumajas, *Pertanggungjawaban Pidana Pelaku Deepfake Porn Menggunakan Artificial Intelligence (AI)*, Jurnal Rectum, Vol.7, No.2 (2025).

C. PENUTUP

Pengaturan hukum di Indonesia terhadap penyalahgunaan *deepfake* AI dalam pornografi digital masih belum memadai. Undang-Undang Pornografi, UU ITE dan KUHP Nasional belum secara eksplisit mengatur produksi dan distribusi konten *deepfake*, sehingga menimbulkan kekosongan hukum (*legal vacuum*). Regulasi yang ada lebih berfokus pada pornografi konvensional, tidak mampu menjangkau karakteristik kejahatan *deepfake* yang non-konsensual, anonim, lintas batas dan sulit pembuktiannya. Pertanggungjawaban pidana pelaku dapat diterapkan secara interpretatif melalui pasal-pasal yang ada, namun menghadapi kendala signifikan, terutama dalam pembuktian *mens rea*, identifikasi pelaku anonim, serta ketiadaan regulasi khusus dan yurisprudensi yang memadai. Akibatnya, terjadi ketidakpastian hukum, kesulitan penegakan hukum dan perlindungan korban yang tidak optimal.

DAFTAR PUSTAKA

Buku

- Brenner, Susan W. 2010. *Cybercrime: Criminal Threats from Cyberspace*. (Santa Barbara: Praeger).
- Casey, Eoghan. 2011. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. (Amsterdam: Academic Press).
- Arief, Barda Nawawi. 2016. *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*. (Jakarta: Prenada Media Group).

Publikasi

- Aikey, Kennedy. *Fabricated Images, Real Harm: The DEFIANCE Act and Federal Civil Remedies for Deepfake Pornography*. University of Cincinnati Law Review Blog. Vol.94 (2026).
- Amelia, Yolanda Frisky, Arfan Kaimuddin dan Hisbul Luthfi Ashsyarofi. *Pertanggungjawaban Pidana Pelaku terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake menurut Hukum Positif Indonesia*. Dinamika: Jurnal Ilmiah Ilmu Hukum. Vol.30. No.1 (2024).
- AR, Aris Munandar, dkk.. *Peran Niat (Mens Rea) dalam Pertanggungjawaban Pidana di Indonesia*. JIMMI: Jurnal Ilmiah Mahasiswa Multidisiplin. Vol.1. No.3 (2024).
- Aruan, Juandry. *Legal Protection for Victims of Photo Abuse through Artificial Intelligence Technology in Pornography Crimes in Indonesia*. Law & Society Review. Vol.5. No.2 (2025).
- Azis, Abdul. *Rekonstruksi Hukum Penyalahgunaan Artificial Intelligence (AI) dalam Konten Kesusilaan dan Pencemaran Nama Baik*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.6. No.7 (2025).
- Chalil, Nurhayati dan Fathurrahim. *Perlindungan Hukum atas Martabat dan Privasi Perempuan dari Praktik Deepfake Pornografi*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.6. No.12 (2025).
- Chesney, Robert dan Danielle Citron. *Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics*. Foreign Affairs. Vol.98. No.1 (2019).
- Citron, Danielle Keats. *Sexual Privacy*. Yale Law Journal. Vol.128. No.7 (2019).
- Fichtner, J. Royce dan Troy J. Strader. *Criminalizing Deepfakes: A Comprehensive Review of US Legislative Responses to Synthetic Media Abuse*. Journal of the Midwest Association for Information Systems. Vol.1. No.3 (2026).
- Franks, Mary Anne. *Sexual Harassment 2.0*. Maryland Law Review. Vol.71. No.3 (2012).
- Ghazmi, Shabrina Fadiah. *Urgensi Pengaturan Artificial Intelligence pada Sektor Bisnis Daring di Indonesia*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.2. No.8 (2021).
- Goodfellow, Ian J, dkk.. *Generative Adversarial Nets*. Prosiding Advances in Neural Information Processing Systems (2014).

Kevin David Sirait, Arman Saut Rivando, Cecilia Angel, Zico Ricardo Aritonang dan Lenny Maria Aritonang

Pertanggungjawaban Pidana atas Deepfake AI dalam Produksi dan Distribusi Pornografi Digital di Indonesia

Greeno, Taylor. *Take It Down or Take it Too Far? The Legal Fallout of New Online Takedown Powers*. North Carolina Journal of Law & Technology. Vol.27. No.2 (2025).

Hifni, Mohammad, Safiulloh dan Mutiara Rizka Azzahra. *Tindak Pidana Pornografi dalam Putusan Pengadilan Negeri Sleman Nomor 220/Pid.Sus/2022/PN Sleman*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.6. No.7 (2025).

Hildebrandt, Mireille. 2020. *Law for Computer Scientists and Other Folk*. (Oxford: Oxford University Press).

Irawati, Nurulhuda, Ismansyah dan Nani Mulyati. *Pertanggungjawaban Pidana Deepfake Porn Berbasis AI: Studi Perbandingan dan Implikasi Global*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.7. No.1 (2026).

Judijanto, Loso, Andrew Shandy Utama dan Heri Setiyawan. *Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia*. The Easta Journal Law and Human Rights. Vol.3. No.2 (2025).

Karo, Rizky Karo, Zein Jiddan dan Hanan Atanto Buono. *Analisis dalam Kasus Penyalahgunaan Deepfake dari Segi Perlindungan Data Pribadi dalam UU ITE dan UU PDP di Indonesia*. Prosiding Seminar Nasional Pendidikan, Ilmu-Ilmu Sosial dan Hukum. Vol.1. No.1 (2026).

Kietzmann, Jan H, dkk.. *Deepfakes: Trick or Treat?*. Business Horizons. Vol.63. No.2 (2020).

Meliana, Yang. *Urgensi Formulasi Perlindungan Hukum dan Kepastian Pidana terhadap Pengaturan Tindak Pidana Deepfake dalam Sistem Hukum Pidana Nasional*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.6. No.7 (2025).

Polandos, Tesalonika Liony, Wenly R. J. Lolong dan Merry Lenda Kumajas. *Pertanggungjawaban Pidana Pelaku Deepfake Porn Menggunakan Artificial Intelligence (AI)*. Jurnal Rectum. Vol.7. No.2 (2025).

Putri, Nabilatul Alimah, Nabilah Nurmasitha dan Ni Luh Neisya. *Analisis Pertanggungjawaban Perdata terhadap Penyalahgunaan Teknologi Artificial Intelligence (Deepfake)*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.6. No.12 (2025).

Respati, Adnasohn Aqilla, dkk.. *Analisis Hukum terhadap Pencegahan Kasus Deepfake serta Perlindungan Hukum terhadap Korban*. Media Hukum Indonesia. Vol.2. No.2 (2024).

Sitanggang, Andri Sahata, Fernanda Darmawan dan Dony Saputra Manurung. *Hukum Siber dan Penegakan Hukum di Indonesia: Tantangan dan Solusi Memerangi Kejahatan Siber*. Jurnal Pendidikan dan Teknologi Indonesia. Vol.4. No.3 (2024).

Sy, Muhammad Faturrachman. *Deepfake Pornografi: Studi Konstitusi dan Penegakannya di Indonesia*. Legislatif. Vol.8. No.2 (2025).

Zumarno, Gefy Caesarati, Sri Jaya Lesmana dan Ratna Indayatun. *Bridging Legal Gaps in AI-Generated Deepfake Pornography: A Comparative Approach to Privacy and Digital Ethics*. Jurnal Ius Constituendum. Vol.11. No.2 (2026).

Website

Yolandha, Friska. *Komdigi Putus Akses Sementara Grok, Lindungi Warga dari Pornografi AI*. diakses dari <https://ameera.republika.co.id/berita/t8msv2370/komdigi-putus-akses-sementara-grok-lindungi-warga-dari-pornografi-ai?>. diakses pada 29 April 2026.

Sumber Hukum

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1. Tambahan Lembaran Negara Republik Indonesia Nomor 6842.

South Korea. *Act on Special Cases Concerning the Punishment of Sexual Crimes*. Pub. L. No.17264 (2020).

Parliament of Australia. *Criminal Code Amendment (Deepfake Sexual Material) Act 2024*. No.78. 2024. Federal Register of Legislation.