

A Legal Analysis of Evidence and Law Enforcement for Victims of Deepfake Pornography in Indonesia

[Analisis Yuridis Pembuktian dan Penegakan Hukum Korban dalam Deepfake Pornografi di Indonesia]

Deva Putra Tegas Sakti¹⁾, Mochammad Tanzil Multazam ^{*,2)}

¹⁾ Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia

²⁾ Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia

*Email Penulis Korespondensi: tanzilmultazam@umsida.ac.id

Abstract. *The misuse of artificial intelligence (AI) technology in the form of deepfake pornography has triggered a serious form of digital sexual violence in Indonesia. This study aims to analyze the legal qualifications, mechanisms of electronic evidence, and the effectiveness of law enforcement available to victims within Indonesia's criminal and civil justice systems. The research method employed is a normative legal approach based on legislation. The primary legal sources used include the Criminal Code, the Criminal Procedure Code, Law No. 1 of 2024 (Second Amendment to the ITE Law), Law No. 44 of 2008 on Pornography, Law No. 12 of 2022 on TPKS, Law No. 27 of 2022 on PDP, and Law No. 28 of 2014 on Copyright. Secondary legal sources include legal textbooks, articles from accredited academic journals, and relevant legal literature. The legal materials were analyzed deductively to logically outline the issues. The research findings indicate that deepfake pornography exhibits the characteristics of a hybrid crime that triggers overlapping norms across various laws. In terms of evidence, the trial process is multi-layered because the validation requirement applies not only to the existence of the content but also to the identification of facial biometric data using facial recognition, as well as digital forensic analysis to identify traces of pixel manipulation. Furthermore, although victims have the option to seek redress through both criminal and civil channels (Lawsuit for Unlawful Acts under Article 1365 of the Civil Code), implementation has not been optimal due to regulatory lag, limited forensic capacity among law enforcement officials, and low digital legal literacy among victims. This study concludes that there is a need for substantive legal reform specifically addressing AI-based crimes and for improved integration of the national digital forensic infrastructure.*

Keywords - deepfake pornography; digital evidence; legal protection; personal data; cybercrime

Abstrak. *Penyalahgunaan teknologi kecerdasan buatan (Artificial Intelligence) dalam bentuk deepfake pornografi telah memicu bentuk kekerasan seksual berbasis digital yang serius di Indonesia. Penelitian ini bertujuan untuk menganalisis kualifikasi hukum, mekanisme pembuktian elektronik, serta efektivitas penegakan hukum yang dapat ditempuh oleh korban dalam sistem peradilan pidana dan perdata di Indonesia. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan. Bahan hukum primer yang digunakan mencakup Kitab Undang-Undang Hukum Pidana (KUHP), Kitab Undang-Undang Hukum Acara Pidana (KUHAP), Undang-Undang Nomor 1 Tahun 2024 (Perubahan Kedua UU ITE), Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, Undang-Undang Nomor 12 Tahun 2022 tentang TPKS, Undang-Undang Nomor 27 Tahun 2022 tentang PDP, dan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta. Bahan hukum sekunder meliputi buku teks hukum, artikel jurnal ilmiah terakreditasi, serta literatur hukum yang relevan. Bahan hukum dianalisis secara deduktif untuk menguraikan permasalahan secara logis. Hasil penelitian menunjukkan bahwa deepfake pornografi memiliki karakteristik kejahatan hibrid yang memicu tumpang tindih norma (overlapping norms) di berbagai undang-undang. Dalam aspek pembuktian, proses di persidangan bersifat multi-layer atau berlapis karena kewajiban validasi tidak hanya tertuju pada eksistensi konten, melainkan pada identifikasi data biometrik wajah menggunakan face recognition serta analisis forensik digital untuk mengidentifikasi jejak manipulasi piksel. Lebih lanjut, meskipun korban memiliki opsi penyelesaian melalui jalur pidana maupun perdata (Gugatan Perbuatan Melawan Hukum Pasal 1365 KUHPerdata), implementasinya belum optimal akibat adanya ketertinggalan regulasi (regulatory lag), keterbatasan kapasitas forensik aparat penegak hukum, serta rendahnya literasi digital hukum dari korban. Penelitian ini menyimpulkan perlunya reformasi hukum materiil yang spesifik mengatur kejahatan berbasis kecerdasan buatan dan peningkatan integrasi infrastruktur forensik digital nasional.*

Kata Kunci - deepfake pornografi; alat bukti elektronik; perlindungan hukum; data pribadi; kejahatan siber

I. PENDAHULUAN

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence/AI*) telah membawa perubahan besar dalam kehidupan digital masyarakat, termasuk dalam produksi dan manipulasi konten visual. Salah satu bentuk teknologi yang berkembang pesat adalah *deepfake*, yaitu teknik manipulasi berbasis *machine learning* yang memungkinkan penggantian wajah seseorang ke dalam tubuh orang lain secara realistis. Memiliki manfaat dalam industri tersebut tidak membuat teknologi ini menjadi selalu dalam arah yang baik, ada kalanya teknologi ini disalahgunakan untuk melanggar hukum seperti pembuatan konten pornografi tanpa persetujuan orang yang ada dalam konten tersebut. Deepfake pornografi kini berkembang menjadi salah satu bentuk baru pelecehan seksual berbasis digital yang menimbulkan berbagai dampak serius bagi para korban.[1]

Munculnya kasus rekayasa digital wajah menunjukkan bahwa kemajuan teknologi belum diiringi dengan kesiapan susunan aturan yang memadai dalam memberikan perlindungan. Korban dalam kasus semacam ini sering mengalami berbagai kerugian, mulai dari rusaknya nama baik, tekanan psikologis, hingga hilangnya kendali atas branding digital pribadi mereka. Meskipun rekayasa digital pornografi menggunakan (*Artificial Intelligence/AI*) tidak selalu menggunakan tubuh asli korban, teknologi tersebut mampu menghasilkan visual yang tampak sangat nyata. Akibatnya, dampak yang dirasakan korban dapat setara bahkan lebih luas dibandingkan kejahatan pornografi konvensional, terutama karena internet dan media sosial memungkinkan penyebaran konten terjadi dengan sangat cepat dan luas. Reproduksi dan penyebaran tanpa batas juga menyebabkan korban sulit menghapus jejak digital secara keseluruhan.

Korban menghadapi kesulitan dalam membuktikan bahwa dirinya adalah korban karena konten yang sudah beredar merupakan hasil manipulasi, pada akhirnya pelaku akan mudah berdalih konten tersebut tidak melibatkan korban secara nyata. Di sisi lain, aparat penegak hukum dihadapkan pada tantangan untuk mengidentifikasi pelaku, membuktikan unsur manipulasi digital, serta mengaitkan perbuatan tersebut dengan norma hukum yang berlaku. Persoalan utama dalam kejahatan *deepfake* pornografi tidak hanya terletak pada aspek pengaturan hukum, tetapi juga pada mekanisme pembuktian dan penegakan hukum yang dapat dilakukan oleh korban untuk memperoleh keadilan.[2]

Penelitian mengenai kekerasan seksual berbasis digital di Indonesia umumnya berfokus pada penyebaran konten pornografi tanpa izin, *revenge porn*, atau pelanggaran kesusilaan melalui media elektronik. Beberapa penelitian juga mengkaji penerapan Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Pornografi dalam menangani kejahatan siber yang berkaitan dengan kesusilaan. Di tingkat internasional, studi mengenai *deepfake* lebih banyak menyoroti aspek teknologi, seperti deteksi konten palsu, dampak terhadap disinformasi, serta ancaman terhadap keamanan digital. Penelitian yang secara khusus membahas *deepfake* pornografi dalam perspektif hukum, khususnya terkait pembuktian dan perlindungan korban masih terbatas. [3]

Penelitian telah mulai mengaitkan *deepfake* dengan isu perlindungan data pribadi, terutama terkait penggunaan data biometrik seperti wajah tanpa persetujuan. Wajah dipandang sebagai bagian dari identitas personal yang memiliki nilai hukum dan harus dilindungi. Meskipun begitu kajian tersebut masih belum menguraikan secara rinci bagaimana korban dapat menggunakan instrumen hukum yang tersedia untuk menuntut haknya. Penelitian mengenai kekerasan seksual berbasis elektronik dalam kerangka Undang-Undang Tindak Pidana Kekerasan Seksual juga masih belum secara spesifik mengakomodasi fenomena manipulasi wajah menggunakan AI dalam konten pornografi.[4]

Berbagai penelitian terdahulu telah mengkaji isu *Deepfake* dalam menegakan hukum, meskipun masing-masing memiliki fokus yang berbeda. Pertama penelitian yang dilakukan oleh Memei Apriana, Fransisco, dan Any Nugroho tahun 2025 dengan judul “ Perlindungan Hukum Bagi Perempuan Korban Tindak Pidana Kejahatan Artificial Intelligence (AI) Deepfake Berdasarkan Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual “ Hasil Penelitian ini Menunjukkan bahwa meskipun UU TPKS telah mengakomodasi kekerasan seksual berbasis elektronik, belum ada regulasi yang secara eksplisit mengatur rekayasa visual AI *deepfake*. Kekosongan hukum ini menyulitkan pembuktian teknis dan penentuan sanksi, sehingga diperlukan harmonisasi undang-undang serta peningkatan kapasitas aparat penegak hukum dalam memahami kejahatan siber berbasis kecerdasan buatan.[5] Penelitian terdahulu kedua yang ditulis oleh Y. Meliana pada tahun 2025 dengan judul “ Urgensi Formulasi Perlindungan Hukum Dan Kepastian Pidana Terhadap Pengaturan Tindak Pidana *Deepfake* Dalam Sistem Hukum Pidana Nasional “ hasil penelitian ini Menegaskan perlunya pembaruan dan formulasi hukum pidana materiil secara khusus untuk menangani manipulasi identitas berbasis *deepfake*. Ketidadaan aturan yang spesifik mengakibatkan ketidakpastian hukum (*legal uncertainty*) dalam menjerat pelaku serta memberikan asas kepastian hukum dalam sistem peradilan pidana nasional.[6] Penelitian terdahulu yang ketiga ditulis oleh Nurul Aulia Fitriani dan Endik Wahyudi pada tahun 2026 dengan judul “ Kebijakan Formulasi Tindak Pidana Deepfake dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Dan Undang-Undang Perlindungan Data Pribadi (UU PDP) Di Indonesia “ hasil penelitian ini menganalisis kebijakan formulasi tindak pidana *deepfake* dengan memanfaatkan dan mengombinasikan instrumen Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Pelindungan Data Pribadi Indonesia.[7]

Penelitian ini memiliki kebaruan (novelty) dibandingkan dengan penelitian terdahulu terdapat perbedaan mendasar antara kajian-kajian tersebut dengan penelitian ini. Jika penelitian terdahulu umumnya berfokus secara parsial pada aspek kriminologis umum, analisis normatif tunggal terhadap Undang-undang Informasi dan Transaksi Elektronik, maupun sebatas mengkaji isu privasi serta perlindungan perempuan secara makro, penelitian ini secara komprehensif mengintegrasikan analisis yuridis antar regulasi (*cross-sectoral/multi-layered analysis*) yang mencakup Undang-Undang Informasi dan Transaksi Elektronik, Undang-undang Pornografi, Undang-undang Tindak Pidana Kekerasan Seksual, Undang-undang Perlindungan Data Pribadi, Undang-undang Hak Cipta, hingga Kitab Undang-undang Hukum Acara Pidana dan Kitab Undang-undang Hukum Pidana. Lebih lanjut, penelitian ini melangkah lebih jauh dengan membedah mekanisme pembuktian elektronik secara teknis khususnya terkait pengamanan rantai bukti siber (*chain of custody*) dan analisis biometrik wajah (*face recognition*) serta mengevaluasi efektivitas opsi penegakan hukum ganda yang dapat ditempuh korban melalui jalur pidana dan gugatan Perbuatan Melawan Hukum (PMH) Pasal 1365 KUHPerdara demi memulihkan kerugian immaterial yang kerap kali terabaikan dalam jalur peradilan konvensional.[8]

Bahwa penelitian saat ini masih memiliki keterbatasan dalam beberapa aspek. Pertama, penelitian lebih banyak menitikberatkan pada aspek normatif atau pengaturan hukum, tanpa mengkaji secara mendalam bagaimana mekanisme pembuktian dalam praktik. Kedua, belum terdapat integrasi analisis antara berbagai instrumen hukum yang relevan, seperti Undang-Undang ITE, Undang-Undang Pornografi, Undang-Undang TPKS, Undang-Undang Hak Cipta, dan Undang-Undang Perlindungan Data Pribadi, dalam konteks penanganan deepfake pornografi. Ketiga, fokus penelitian masih cenderung pada pelaku atau perbuatan, bukan pada posisi korban dan penegakan hukum yang dapat ditempuh untuk memperoleh keadilan.

Terdapat kesenjangan (gap) penelitian yang signifikan, yaitu belum adanya kajian menyeluruh yang membahas penegakan hukum korban dan pembuktian dalam tindak pelecehan seksual berbasis digital melalui manipulasi wajah (*deepfake* pornografi). Aspek pembuktian merupakan unsur yang sangat penting dalam proses penegakan hukum karena menjadi dasar untuk menentukan apakah suatu perbuatan dapat dikategorikan sebagai tindak pidana serta apakah pelakunya dapat dimintai pertanggungjawaban secara hukum. Selain itu, korban juga memiliki hak untuk menempuh jalur perdata guna mengajukan tuntutan ganti rugi atas kerugian yang dialami.[9] Namun demikian, mekanisme penyelesaian melalui jalur perdata tersebut masih belum banyak dikaji dalam penelitian sebelumnya.

Pembahasan dari penelitian ini mengambil dari contoh kasus yang beredar di sosial media maupun berita televisi karena adanya indikasi yang kuat seiring meningkatnya penggunaan teknologi kecerdasan buatan (AI) dalam kehidupan sehari-hari yang memiliki potensi disalahgunakan untuk tindakan melawan hukum. Tanpa adanya regulasi yang jelas mengenai mekanisme pembuktian dan penegakan hukum yang tersedia, dapat menyebabkan banyak korban penyalahgunaan teknologi kecerdasan buatan akan berada pada posisi yang rentan dan mengalami kesulitan dalam mendapatkan hak perlindungan hukum yang optimal. Penelitian ini juga memiliki harapan yang dapat memberikan kontribusi terhadap perkembangan susunan hukum di Indonesia, khususnya dalam menghadapi penyalahgunaan konten digital yang terus berkembang cepat saat ini. Penelitian ini dapat membantu atau membuka wawasan langsung bagi aparat penegak hukum, kelompok akademis, maupun masyarakat umum karena memberikan gambaran mengenai langkah-langkah hukum yang dapat ditempuh korban dalam menghadapi tindak kejahatan rekayasa digital (*deepfake* pornografi).[10]

Tujuan dari penelitian ini adalah untuk menganalisis penegakan hukum dan mekanisme pembuktian yang dapat dilakukan oleh korban dalam tindak pelecehan seksual berbasis digital melalui manipulasi wajah (*deepfake*) dalam hukum Indonesia, dengan mengkaji penerapan berbagai peraturan perundang-undangan yang relevan serta menilai efektivitasnya dalam memberikan perlindungan hukum bagi korban.

Urgensi Penelitian yaitu melihat dari Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence/AI*) saat ini berkembang sangat cepat dan membawa dampak besar dalam kehidupan sehari-hari. Salah satu hasil teknologinya adalah *deepfake*, yaitu kemampuan merekayasa foto, suara, hingga video seseorang agar terlihat sangat nyata padahal sepenuhnya palsu. Sayangnya, teknologi canggih ini makin sering disalahgunakan untuk tindakan kejahatan, mulai dari penipuan hingga pembuatan konten pornografi palsu tanpa persetujuan korban. Masalah ini bukan lagi sekadar isu teknologi, melainkan sudah menjadi ancaman nyata bagi keselamatan, nama baik, dan keadilan masyarakat. Oleh karena itu, penelitian mengenai penyalahgunaan *deepfake* dari kacamata hukum pidana menjadi sangat penting dan mendesak untuk dilakukan. Ada empat alasan utama mengapa topik ini harus segera dikaji:

1. Aturan Hukum Saat Ini Belum Pas dan Masih Banyak Celah

Prinsip utama hukum pidana kita menegaskan bahwa seseorang baru bisa dihukum jika aturan hukumnya sudah ada dan jelas (*asas legalitas*). Masalahnya, undang-undang yang kita miliki saat ini seperti Undang-Undang ITE, Undang-undang Pornografi, Undang-undang Perlindungan Data Pribadi, Undang-undang Hak Cipta, maupun Undang-undang Tindak Pidana Kekerasan Seksual dibuat sebelum teknologi rekayasa wajah/suara berbasis AI (*deepfake*) ini populer. Akibatnya, hukum kita gagap dan mengalami "kosong aturan" (*legal gap*). Memaksa pasal-pasal lama untuk menjerat pelaku *deepfake* justru berisiko membuat hukum menjadi tebak-tebak buah manggis dan tidak adil.[11]

2. Sulit Menentukan Siapa yang Harus Bertanggung Jawab Dalam teknologi *deepfake*, proses kejahatannya sering kali berantai. Ada orang yang membuat gambarnya, ada yang menyebarkan di media sosial, dan ada aplikasi/platform AI yang menyediakan alatnya. Dalam hukum pidana, kita harus membuktikan niat jahat (*mens rea*) dari masing-masing pihak. Penelitian ini penting untuk memperjelas siapa yang benar-benar harus dihukum dan seberapa besar tanggung jawab hukum mereka.
3. Tantangan Membuktikan Mana yang Asli dan Mana yang Palsu di Pengadilan
Teknologi AI saat ini sudah sangat canggih hingga hasil rekayasanya sulit dibedakan dari video atau foto asli. Di dalam persidangan, polisi dan jaksa butuh bukti yang sah dan tidak terbantahkan. Jika tidak ada standar teknis dan prosedur hukum yang jelas untuk memeriksa keaslian bukti digital, orang yang tidak bersalah bisa dituduh pelaku, atau sebaliknya, pelaku kejahatan bisa lolos dari hukuman karena buktinya dianggap ragu-ragu.[12]
4. Fokus Melindungi dan Memulihkan Nama Baik Korban
Kejahatan *deepfake* terutama yang bermuatan pornografi palsu sangat merusak kehidupan, nama baik, dan mental korbannya (yang mayoritas adalah perempuan). Hukum pidana tidak boleh hanya sibuk memenjarakan pelaku, tetapi juga harus memikirkan nasib korban. Penelitian ini mendesak untuk mencari cara agar foto/video palsu korban bisa langsung dihapus dari internet dan korban mendapat ganti rugi atas kerugian yang dialaminya.

II. METODE

Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan. Bahan hukum primer yang digunakan mencakup Kitab Undang-Undang Hukum Pidana (KUHP), Kitab Undang-Undang Hukum Acara Pidana (KUHPA), Undang-Undang Nomor 1 Tahun 2024 (Perubahan Kedua UU ITE), Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta. Bahan hukum sekunder seperti buku, jurnal ilmiah, dan literatur terdahulu yang masih relevan. Semua data dikumpulkan lewat studi kepustakaan. Analisis bahan hukum dilakukan secara deduktif dengan menggunakan penafsiran gramatikal dan penafsiran sistematis. Penafsiran gramatikal digunakan untuk memahami makna norma berdasarkan rumusan bahasa dalam peraturan perundang-undangan, sedangkan penafsiran sistematis digunakan untuk menghubungkan ketentuan dalam KUHP, KUHPA, Undang-Undang ITE, Undang-Undang Pornografi, Undang-Undang TPKS, Undang-Undang Perlindungan Data Pribadi, dan Undang-Undang Hak Cipta sehingga diperoleh pemahaman yang utuh mengenai mekanisme pembuktian dan penegakan hukum terhadap tindak pidana *deepfake* pornografi.

III. HASIL DAN PEMBAHASAN

A. Kualifikasi Hukum Tindak Deepfake Pornografi dalam Hukum Indonesia

Kemunculan pornografi berbasis kecerdasan buatan (*Artificial Intelligence/AI*) melalui teknologi *deepfake* benar-benar mengguncang konstruksi hukum pidana konvensional kita. Kejahatan ini tidak bisa lagi disamakan dengan pelanggaran kesusilaan biasa di dunia nyata, melainkan merupakan bentuk kejahatan gabungan (*complex crime*) di mana pelaku memalsukan data digital, mencuri data biometrik wajah seseorang tanpa izin, serta menghancurkan nama baik dan hak privasi korban (*digital character assassination*). Karena belum ada undang-undang khusus yang secara eksplisit menyebutkan istilah *Artificial Intelligence* atau *Deepfake*, timbul anggapan keliru di masyarakat bahwa telah terjadi kekosongan hukum di Indonesia. Padahal, hambatan utamanya bukanlah ketiadaan

aturan, melainkan keterlambatan hukum mengejar perkembangan teknologi (*regulatory lag*) serta tumpang tindihnya aturan (*overlapping norms*) yang kerap memicu kebingungan aparat penegak hukum dalam menentukan instrumen undang-undang yang paling tepat untuk digunakan.[12] Secara doktrinal dan yuridis formal, *deepfake* pornografi pada dasarnya secara sah dapat dikualifikasikan sebagai tindak pidana pornografi di dalam sistem hukum pidana Indonesia. Berdasarkan Pasal 1 angka 1 Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, konten *deepfake* memenuhi definisi pornografi karena pembentuk undang-undang tidak membatasi objek hanya pada rekaman tubuh manusia asli, melainkan mencakup perluasan bentuk media seperti "gambar bergerak, animasi, kartun, atau bentuk pesan lainnya" yang memuat kecabulan atau eksploitasi seksual. Dalam hukum pidana, fokus penilaian tidak terletak pada keaslian fisik objeknya, melainkan pada niat jahat (*mens rea*) dan perbuatan nyata (*actus reus*) pelaku. Oleh karena itu, tindakan memproduksi, membuat, maupun menggandakan *deepfake* pornografi terbukti melanggar Pasal 4 ayat (1) jo. Pasal 29 Undang-Undang Pornografi dengan ancaman pidana penjara hingga 12 tahun dan denda paling banyak Rp6 Miliar. Meski demikian, penanganan kejahatan siber ini tidak boleh berhenti pada Undang-Undang Pornografi semata yang cenderung terfokus pada pemidanaan pelaku dan mengabaikan nasib korban. Ketentuan normatif Undang-Undang Pornografi tersebut wajib diselaraskan dan digabungkan secara serentak dengan aturan lain, seperti Pasal 14 UU No. no 12 tahun 2022 Undang-Undang Tindak Pidana Kekerasan Seksual terkait Kekerasan Seksual Berbasis Elektronik, Pasal 27 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik mengenai perbuatan asusila di ruang siber, Undang-Undang no 28 tahun 2024 tentang Hak cipta, serta Undang-Undang Perlindungan Data Pribadi. Dengan mengintegrasikan seluruh aturan hukum siber, perlindungan data pribadi, hingga hukum Tindak Pidana Kekerasan Seksual, penegak hukum tidak hanya dapat menjerat seluruh tingkatan perbuatan pelaku secara komprehensif, tetapi juga mampu memberikan kepastian hak restitusi (ganti rugi) serta pemulihan psikologis bagi korban secara menyeluruh. Dengan memetakan semua aturan ini secara jelas, hambatan dan kebingungan antar aturan dapat diselesaikan. Tabel di bawah ini merangkum bagaimana gabungan berbagai aturan hukum di Indonesia saling melengkapi untuk menjerat kasus *deepfake* pornografi:

Tabel 1. Pemetaan Instrumen Hukum dalam Penanganan Kasus Deepfake Pornografi di Indonesia

NO	Instrumen Hukum / Regulasi.	Pasal & Unsur Delik Relevan.	Isu Yuridis Khusus dalam Kasus <i>Deepfake</i> .	Peran Konkret bagi Pemulihan / Perlindungan Korban.
1.	Kitab Undang-Undang Hukum Pidana (KUHP)	asal 408 KUHP (Pencemaran nama baik), Pasal 414 KUHP (Fitnah)	Berperan sebagai <i>subsidiaritas</i> (pembantu hukum) jika pola kejahatan meluas ke dunia nyata (misalnya mencetak tangkapan layar <i>deepfake</i> untuk teror fisik).	Menjerat motif pelaku yang sengaja menyerang kehormatan, memeras, atau menghancurkan reputasi sosial korban di lingkungan nyata.
2.	Kitab Undang-Undang Hukum Acara Pidana (KUHAP)	Pasal 184 ayat (1) KUHAP	Menjawab tantangan <i>scientific crime investigation</i> . Hakim mewajibkan analisis <i>multi-layered</i> menggunakan <i>digital forensic</i> dan <i>face recognition</i> .	Mengawal agar <i>chain of custody</i> (rantai pengamanan bukti siber) tetap sah, sehingga kasus tidak gugur (<i>false negative</i>) akibat bukti digital yang dianggap cacat hukum.
3.	UU No. 1 Tahun 2024 (UU ITE Kedua)	Pasal 35 jo. 51 ayat (1): Manipulasi data agar dianggap otentik.	<i>Regulatory lag</i> pada AI diatasi dengan delik rekayasa digital (<i>data forgery</i>). Fokusnya membuktikan niat jahat (<i>mens rea</i>)	Menjadi dasar hukum utama untuk menuntut <i>take-down</i> (penghapusan) konten di internet guna memutus

		Pasal 27 ayat (1): Distribusi konten melanggar kesusilaan.	pelaku untuk memalsukan identitas korban.	penyebaran jejak digital korban.
4.	UU No. 27 Tahun 2022 (UU Perlindungan Data Pribadi / PDP)	Pasal 4 ayat (2), Pasal 65 <i>jo</i> . Pasal 67: Pemrosesan dan penyalahgunaan data pribadi spesifik tanpa hak.	Wajah korban diklasifikasikan sebagai Data Biometrik. Proses <i>training</i> AI menggunakan wajah korban tanpa izin (<i>consent</i>) dinilai sebagai pelanggaran kedaulatan data.	Menjamin hak otonomi korban atas tubuh digitalnya serta memberikan sanksi pidana/denda besar bagi korporasi atau individu pemilik platform pembuat <i>deepfake</i> .
5.	UU No. 12 Tahun 2022 (UU Tindak Pidana Kekerasan Seksual / TPKS)	Pasal 14: Kekerasan Seksual Berbasis Elektronik (KSBE).	Mengakomodasi dimensi kekerasan gender nonfisik di mana visualisasi seksual diproduksi di luar kehendak korban.	Sangat Progresif: Memberikan hak atas Restitusi (ganti rugi materiil dari pelaku), pendampingan psikologis (LPSK), perlindungan dari kriminalisasi balik.[13]
6.	UU No. 44 Tahun 2008 (UU Pornografi)	Pasal 4 ayat (1): Larangan memproduksi, membuat, atau menggandakan pornografi.	Mengatasi perdebatan <i>fictional pornography</i> . Visualisasi AI dinilai tetap melanggar asusila karena publik mengasosiasikan visual tersebut sebagai korban secara riil.	Memberikan legitimasi hukum bahwa martabat kemanusiaan korban telah dilecehkan secara visual di muka publik meskipun tubuh fisiknya tidak terlibat langsung.
7.	UU No. 28 Tahun 2014 (UU Hak Cipta)	Pasal 12 & Pasal 115: Larangan penggunaan potret seseorang untuk komersial/pengumuman tanpa izin tertulis.	Menjerat tindakan pemanenan foto komersial/pribadi korban (dari Instagram/LinkedIn) yang dimodifikasi secara ilegal demi keuntungan ekonomi pelaku.	Memberikan peluang bagi korban untuk menuntut ganti rugi materiil atas pelanggaran Hak Potret (<i>Right to Image</i>) jika video <i>deepfake</i> dijual di platform berbayar.

Sumber : Dari Penulis

Berdasarkan pemetaan antar regulasi pada tabel 1, analisis diatas menunjukkan adanya fenomena *overlapping norms* (tumpang tindih norma) yang sangat kompleks dalam sistem hukum positif Indonesia saat menghadapi kejahatan berbasis kecerdasan buatan. Jika dibedah secara struktural, penegakan hukum kasus *deepfake* pornografi tidak dapat diselesaikan secara parsial karena melibatkan tiga lapisan perlindungan hukum yang saling berkelindan, yaitu siber data, konten pornografi, dan pemulihan korban.

B. Mekanisme Pembuktian oleh Korban dalam Deepfake Pornografi

Beralih ke pembuktian di dalam persidangan, kunci utama untuk menentukan pelaku bersalah atau tidak terletak pada kekuatan pembuktian. Kejahatan *deepfake* pornografi memberikan tantangan besar bagi sistem pembuktian konvensional yang diatur dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHP). Sistem pembuktian konvensional dalam KUHP biasanya digunakan untuk kejahatan yang meninggalkan barang bukti fisik yang kelihatan (seperti surat, benda, atau sidik jari). Sementara itu, barang bukti kejahatan *deepfake* berbasis (AI)

bersifat digital, sangat mudah diubah tanpa jejak, dan rentan rusak keasliannya jika tidak ditangani dengan prosedur yang benar. Karena itu, penyidikan tidak bisa lagi dengan cara lama, melainkan harus menggunakan penyidikan berbasis ilmiah (*scientific crime investigation*). [14] Di ruang sidang, hambatan terbesar bagi Jaksa Penuntut Umum untuk meyakinkan Hakim adalah pembelaan dari Terdakwa. Terdakwa dengan mudah dapat berdalih bahwa akunnya diretas, atau video tersebut dibuat secara otomatis oleh sistem tanpa ada niat jahat (*mens rea*) darinya. Jika Jaksa hanya mengandalkan bukti cetak (*print-out*) berupa kertas hasil *screenshot*, Terdakwa bisa lolos dari hukuman (mendapat putusan bebas). Dalam hukum siber, kertas *screenshot* tidak dianggap sebagai bukti yang kuat karena sudah terpisah dari sistem digital aslinya. Untuk memastikan bukti digital itu sah menurut Undang-Undang ITE, penegak hukum wajib menjaga rantai pengamanan bukti siber (*chain of custody*). Artinya, sejak HP atau komputer disita, jaringan internetnya harus dimatikan agar data tidak dihapus dari jauh, kode unik filenya (nilai *hash*) harus dicatat, hingga diperiksa di laboratorium forensik siber. [15] Jika ada satu langkah saja yang terlewat, bukti tersebut bisa dinyatakan tidak sah oleh Hakim karena dianggap sudah terkontaminasi. Selain itu, menentukan keaslian video tidak boleh hanya dikira-kira dengan mata telanjang. Laboratorium forensik digital harus membuktikannya secara ilmiah melalui analisis pencahayaan wajah dan deteksi algoritma menggunakan teknologi *face recognition*. Di sinilah Alat Bukti Keterangan Ahli forensik digital berperan sangat penting untuk menjelaskan data teknologi yang rumit kepada Majelis Hakim. Keterangan Ahli inilah yang memperkuat Alat Bukti Surat (berupa Laporan Hasil Pemeriksaan Forensik Digital) yang menjadi dasar bagi Hakim untuk menyusun Alat Bukti Petunjuk hingga meyakini kesalahan Terdakwa. maka berikut ini disajikan rekonstruksi ilmiah dalam bentuk Tabulasi Konstruksi Alat Bukti dan Prosedur Uji Forensik Kasus *Deepfake* Pornografi:

Tabel 2. Konstruksi Alat Bukti dan Prosedur Uji Forensik pada Kasus *Deepfake* Pornografi

N O	Alat Bukti (Pasal 184 KUHP)	Manifes Teknis / Objek <i>Deepfake</i>	Prosedur <i>Chain of Custody</i> & Metode Forensik	Parameter Keabsahan Yuridis di Persidangan	Titik Celah Hukum (<i>Defense Mechanism</i>) & Cara Mitigasi
1.	Keterangan Ahli (Pasal 184 ayat 1 huruf b KUHP)	Ahli <i>Digital Forensics</i> Ahli Kedokteran Kehakiman (Biometrik Wajah) Ahli Hukum Siber	Pemeriksaan dilakukan terhadap klon digital (<i>bit-stream image</i>) dari perangkat sitaan menggunakan metode <i>write-blocker</i> agar data asli tidak termodifikasi. Penerapan metode <i>Deep Learning Detektor</i> untuk memeriksa inkonsistensi spasial dan temporal berkas video.	Pemenuhan kualifikasi formal ahli (Sertifikasi CHFI/CEH atau akademisi bereputasi). Penyampaian Laporan Hasil Pemeriksaan Forensik Digital (LHPFD) di bawah sumpah persidangan.	Celah: Penasihat hukum menuduh metode deteksi ahli bersifat eksperimental. Mitigasi: Ahli wajib mendasarkan metodologinya pada standar internasional ISO/IEC 27037 terkait penanganan bukti digital.
2.	Surat (Pasal 184 ayat 1 huruf c KUHP)	LHPFD dari Puslabfor Polri.	Diterbitkan secara resmi oleh institusi forensik negara atau ahli independen yang	Keotentikan tanda tangan ahli secara fisik/elektronik. Surat memuat rincian ilmiah matematis	Celah: Surat dianggap cacat formal jika <i>tools</i> ekstraksi forensik tidak terkalibrasi. Mitigasi: Melampirkan sertifikat kalibrasi perangkat

		Sertifikat Digital Forensik. Lembar Hasil Perbandingan Dokumen Biometrik Wajah.	ditunjuk oleh ketetapan hakim. Penyusunan kronologis dokumen mencakup metode, alat (<i>tools</i>), dan hasil nilai logika pembuktian.	mengenai nilai <i>hash</i> (MD5/SHA-256) berkas video sebelum dan sesudah dianalisis.	lunak forensik (misal: EnCase/Cellebrite) dalam lampiran berkas perkara.
3.	Petunjuk (Pasal 184 ayat 1 huruf d KUHP)	Persesuaian antara <i>digital footprint</i> (jejak digital) pelaku dengan kerugian korban.	Hakim menyusun konklusi berdasarkan persesuaian antara keterangan saksi, keterangan ahli, dan barang bukti elektronik yang dihadirkan.[16] Analisis riwayat unduhan wajah korban pada gawai pelaku.	Hanya bisa ditarik oleh Hakim dalam sidang musyawarah. Harus didasarkan pada logika hukum yang rasional, bukan asumsi normatif semata.	Celah: Penasihat hukum memotong kausalitas dengan dalih gawai pelaku dipinjam orang lain. Mitigasi: Menunjukkan kecocokan koordinat GPS log lokasi gawai, alamat IP, dan <i>timestamp</i> aktivitas saat video dibuat.
4.	Keterangan Terdakwa (Pasal 184 ayat 1 huruf e KUHP)	Pengakuan atau penyangkalan pelaku atas pengoperasian algoritma <i>deepfake</i> .	Pemeriksaan verbal yang dituangkan dalam BAP Tersangka oleh penyidik dengan mematuhi hak-hak tersangka (tanpa tekanan/paksaan) . [17]	Pengakuan terdakwa hanya mengikat dirinya sendiri dan harus diperkuat oleh alat bukti sah yang lain (<i>corroborative evidence</i>).	Celah: Terdakwa mencabut BAP di persidangan dengan alasan mendapat tekanan psikologis. Mitigasi: Jaksa tidak boleh bergantung pada pengakuan pelaku, melainkan memperkuat rantai bukti teknis digital (<i>unbreakable digital chain</i>).
5.	Bukti Elektronik (Perluasan UU ITE & UU TPKS)	Berkas video manipulasi (.mp4/.mkv). Gambar / berkas foto manipulasi (jpg, png) Struktur <i>metadata</i> dan	Langkah Krusial Korban: Pengamanan bukti awal (<i>preservation</i>) 1. Bukti berkas pada Perangkat mengamankan file master asli (dari	Informasi Elektronik dinyatakan sah jika dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan (Pasal 5 & 6 UU ITE).	Celah: <i>Metadata</i> video dinilai rusak akibat proses kompresi otomatis platform (misal: WhatsApp, Instagram/Telegram) atau tautan/URL diblokir/dihapus pelaku sebelum disita. Mitigasi: Penyidik wajib melacak <i>file master</i> asli dari media penyimpanan lokal pelaku (<i>cache/local storage</i>) atau <i>server log</i> pengunggah

		log transmisi siber. Jejak <i>URL/URI, IP Address</i>, serta <i>cache</i> lokal/memori sementara pada Hp, Tablet, Laptop, Komputer	penyimpanan lokal atau <i>cache</i> gawai) atau melakukan Ekspor resmi data platform (<i>Native Platform Export</i>) untuk mengunci nilai <i>hash</i> aslinya sebelum terkompresi oleh sistem WhatsApp Instagram atau Telegram. Penyitaan gawai wajib disertai izin Ketua Pengadilan Negeri setempat guna memenuhi asas <i>due process of law</i>. [19] 2. Bukti berupa URL/ Tautan Aktif Melakukan <i>Web Archiving</i> (misal via <i>web.archive.org</i> atau <i>archive.today</i>) untuk mengunci tampilan dan konten sebelum dihapus oleh pelaku/platform. Mengunduh halaman web beserta berkas media dalam format <i>WARC/HTML</i> utuh. Mencatat <i>metadata URL, IP Address</i> server <i>hosting</i>, serta <i>timestamp</i> (zona waktu) secara presisi.	Nilai <i>hash</i> barang bukti konstan dari tahap penyitaan hingga persidangan.	pertama, serta melampirkan berkas <i>Web Archiving</i> (.warc) dan catatan nilai <i>hash</i> SHA-256 awal dari URL tersebut. [18]
--	--	--	---	--	--

			Menghasilkan nilai <i>hash</i> (SHA-256) terhadap berkas arsip web tersebut guna mengunci keutuhan data (<i>integrity</i>). [20]	
--	--	--	--	--

Sumber : Dari Penulis

Jika rincian alat bukti pada tabel 2 kita bedah lebih dalam, terlihat jelas adanya perubahan besar dalam cara hukum acara pidana kita menilai kekuatan bukti di pengadilan. Kehadiran teknologi seperti *deepfake* memaksa sistem peradilan untuk tidak lagi hanya bergantung pada bukti fisik yang kelihatan saja. Bukti digital itu tidak berwujud dan sangat mudah diubah atau dimanipulasi. Artinya, sebuah video rekayasa AI diakui sah atau tidaknya oleh hakim bukan cuma dilihat dari apa yang tampak di layar, melainkan dari bagaimana bukti digital itu dijaga dan diamankan sejak awal ditemukan (*chain of custody*). Dalam persidangan, penggabungan antara Kitab Undang-Undang Hukum Pidana (KUHP), Kitab Undang-Undang Hukum Acara Pidana (KUHAP), undang-undang Informasi dan transaksi elektronik (ITE), undang-undang perlindungan data pribadi, undang-undang pornografi, undang-undang hak cipta, atau undang-undang tindak pidana kekerasan seksual. ini berfungsi sebagai perisai untuk mematahkan alasan atau pembelaan dari terdakwa. Sering kali pengacara terdakwa berusaha meloloskan kliennya dengan alasan data video sudah rusak saat dikirim via WhatsApp atau Telegram. Nah, untuk menjawab alasan tersebut, jaksa bisa mengajukan bukti berlapis berbasis sains dan teknologi. Disinilah Alat Bukti Keterangan Ahli forensik digital memegang peranan sangat penting. Melalui pemeriksaan kode unik file (nilai *hash* yang berfungsi sebagai "sidik jari digital") serta analisis bentuk wajah (*face recognition*), ahli forensik dapat menerbitkan Alat Bukti Surat berupa Laporan Hasil Pemeriksaan Forensik Digital (LHPFD) yang sah secara ilmiah. Pada akhirnya, bukti-bukti elektronik yang diatur dalam undang-undang tidak akan ada artinya jika tidak ada logika yang kuat untuk meyakinkan hakim. Laporan forensik dari ahli inilah yang menjadi jembatan untuk menghubungkan jejak digital pelaku dengan kerugian nyata yang dialami korban. Jika pengamanan bukti digital dilakukan dengan disiplin dan didukung sains yang akurat, alasan bohong dari terdakwa bisa dipatahkan, sehingga risiko pelaku lolos dari hukuman (*putusan bebas*) dapat dicegah dan keadilan bagi korban benar-benar terwujud.

IV. SIMPULAN

Melalui metode penelitian dengan menguji undang-undang yang berlaku, penelitian ini membuktikan bahwa kasus *deepfake* pornografi bukan sekadar pelanggaran kesusilaan biasa. Kejahatan ini adalah bentuk kejahatan siber kompleks yang merusak perlindungan hak privasi dan nama baik seseorang di Indonesia. Kajian mendalam terhadap undang-undang yang berlaku saat ini menunjukkan adanya aturan yang saling tumpang tindih serta kekosongan aturan hukum. Sebab, undang-undang yang ada saat ini seperti Kitab Undang-Undang Hukum Pidana (KUHP), Kitab Undang-Undang Hukum Acara Pidana (KUHAP), undang-undang Informasi dan transaksi elektronik (ITE), undang-undang perlindungan data pribadi, undang-undang pornografi, undang-undang hak cipta, atau undang-undang tindak pidana kekerasan seksual. belum secara khusus mengatur tindakan rekayasa foto/video berbasis (*AI*) yang dibuat tanpa izin korban. Akibatnya, timbul hambatan besar dalam proses sidang di pengadilan, terutama mengenai siapa yang wajib membuktikan dan bagaimana menentukan keaslian bukti digital. Hal ini terjadi karena cara pembuktian lama kita masih bersandar pada bukti-bukti fisik. Dari sisi teori, penelitian ini memberi masukan bagi pembaruan aturan hukum pidana agar tidak tertinggal oleh perkembangan teknologi, serta memberikan kejelasan tentang siapa saja yang bisa dihukum pidana dalam penggunaan teknologi AI. Dari sisi praktik, penelitian ini menjadi panduan praktis bagi korban untuk melakukan pencegahan dan perlindungan hukum sejak awal. Selain itu, penelitian ini menjadi panduan bagi polisi dan jaksa untuk memanfaatkan jalur Gugatan Perbuatan Melawan Hukum (Pasal 1365 KUHPerdata) sebagai cara tambahan untuk menuntut ganti rugi atas kerugian nama baik dan mental korban yang sering terabaikan di sidang pidana biasa. Sebagai penutup, penelitian ini mendesak perlunya pembaruan undang-undang secara menyeluruh, Baik dengan membuat undang-undang baru atau mengubah aturan yang ada untuk tegas mempidanakan pelaku rekayasa digital. Langkah ini harus didukung dengan standar pemeriksaan forensik digital

nasional berbasis pengenalan wajah (*face recognition*), peningkatan kemampuan penegak hukum, serta peningkatan pemahaman hukum digital bagi masyarakat agar tidak ada lagi pelaku kejahatan yang lolos dari hukuman.

UCAPAN TERIMA KASIH

Alhamdulillah, Penulis mengucapkan terima kasih kepada Universitas Muhammadiyah Sidoarjo atas dukungan akademik, penyediaan sarana dan prasarana, serta suasana pembelajaran yang mendukung sehingga penelitian dan penyusunan karya ilmiah ini dapat terselesaikan dengan baik.

REFERENSI

- [1] H. Prayoga dan H. Tuasikal, “Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia,” *Abdurrauf Law and Sharia*, vol. 2, no. 1, hlm. 22–38, Mei 2025, doi: <https://doi.org/10.70742/arlash.v2i1.194>
- [2] Fabrizio Richardo Marvil Wanggai, Made Sugi Hartono, dan Ni Putu Ega Parwati, “Analisis Normatif terhadap Penyebaran Deepfake Sebagai Bentuk Kejahatan Siber di Indonesia,” *Majelis: Jurnal Hukum Indonesia*, vol. 3, no. 1, hlm. 122–130, Feb 2026, doi: <https://doi.org/10.62383/majelis.v3i1.1509>
- [3] I. Leliana, G. Irhamdhika, A. Haikal, R. Septian, dan E. Kusnadi, “Etika dalam Era Deepfake: Bagaimana Menjaga Integritas Komunikasi.” *Visikom*, vol. 22, no. 02, pp. 234–243, Jan. 2024. doi: <https://doi.org/10.22441/visikom.v22i02.24229>
- [4] Cerens Amanda Gea Pitaloka, “Penyalahgunaan Teknologi Deepfake untuk Konten Pornografi Non-Konsensual di Indonesia,” *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora*, vol. 2, no. 2, hlm. 74–81, Apr 2025, doi: <https://doi.org/10.62383/humif.v2i2.1475>
- [5] Memei Apriana, Fransisco, and Any Nugroho, “Perlindungan Hukum Bagi Perempuan Korban Tindak Pidana Kejahatan Artificial Intelegent (AI) Deepfake Berdasarkan Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual ”, *JSER*, vol. 7, no. 1, pp. 57-75, Apr. 2025. <https://doi.org/10.54783/jsr.v7i1.796>
- [6] Y. Meliana, “Urgensi Formulasi Perlindungan Hukum dan Kepastian Pidana terhadap Pengaturan Tindak Pidana Deepfake dalam Sistem Hukum Pidana Nasional”, *jhlgl*, vol. 6, no. 7, Jun 2025. doi: <https://doi.org/10.56370/jhlgl.v6i7.1087>
- [7] Nurul Aulia Fitriani dan Endik Wahyudi, “Kebijakan Formulasi Tindak Pidana Deepfake Dalam Undang-Undang Informadi dan Transaksi Elektronik (UU ITE) Dan Undang-Undang Perlindungan Data Pibadi (UU PDP) Di Indonesia,” *Jurnal Hukum to-ra : Hukum Untuk Mengatur dan Melindungi Masyarakat*, vol. 12, no. 1, hlm. 157–169, Apr 2026, doi: <https://doi.org/10.55809/tora.v12i1.647>
- [8] C. T. Noerman and A. L. Ibrahim, “Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara”, *JULR*, vol. 7, no. 2, pp. 603–621, Jun. 2024, doi: <https://doi.org/10.26623/julr.v7i2.8995>
- [9] Maria Karunia Putri Maan, Heryanto Amalo, dan Ngongo Dede, “Analisis Perlindungan Hukum terhadap Penyimpangan Artificial Intelligence dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana,” *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora*, vol. 4, no. 1, hlm. 296–307, Jan 2025, doi: <https://doi.org/10.55606/jurish.v4i1.5071>
- [10] S. J. Al-Ayoubi and M. A. Suharto, “Pemidanaan Kepada Pelaku Konten Pornografi Menggunakan Aplikasi Deepfake Pada Peraturan Perundang-Undangan di Indonesia”, *UNESREV*, vol. 8, no. 1, pp. 163–173, Sep. 2025, doi: <https://doi.org/10.31933/unesrev.v8i1.2464>
- [11] Niken Fernanda, Efi Lailatun Nisfah, Essa Hertiana, dan Tasya Fatah Putri Irawan, “Perlindungan Korban dalam Tindak Pidana Kekerasan Seksual,” *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, vol. 3, no. 2, hlm. 1041–1050, Mei 2025, doi: <https://doi.org/10.61104/alz.v3i2.1268>
- [12] A. Z. Nirmala dan Nunung Rahmania, “Transformasi Bentuk Pelecehan Seksual Dalam Era Kecerdasan Buatan: Tinjauan Hukum Indonesia,” *Unizar Law Review*, vol. 8, no. 1, hlm. 77–90, Jun 2025, doi: <https://doi.org/10.36679/ulr.v8i1.96>
- [13] S. D. Diputra, “Tinjauan Yuridis Terhadap Penerapan Undang-Undang Tindak Pidana Kekerasan Seksual Dalam Kasus Kekerasan Berbasis Digital di Indonesia,” *Jurnal Legalitas*, vol. 2, no. 2, hlm. 83–92, Jul 2024, doi: <https://doi.org/10.58819/jle.v2i2.168>

- [14] D. T. Wicaksono, Niken Putri Lestari, and Friyandi Prasetya, “Penegakan Hukum Pelaku Tindak Pidana Artificial Intelligence (Deepfake) Dalam Perspektif Hukum Positif Indonesia”, *Jurnal Fakta Hukum*, vol. 4, no. 2, pp. 63–70, Mar. 2026. doi: <https://doi.org/10.58819/jfh.v4i2.233>
- [15] S. Nurkholisah, D. Rismana, A. E. Nugroho, A. Munjiyah, dan Q. Ayunisa, “Tantangan Kriminalisasi Deepfake dalam Hukum Pidana Indonesia Challenges in Criminalizing Deepfakes under Indonesian Criminal Law,” *Jurnal USM Law Review*, vol. 8, 2025, doi: <https://doi.org/10.26623/julr.v8i3.13060>
- [16] M. Y. Aldianto and R. R. Phahlevy, “Hak Remisi bagi Narapidana Pasca Amandemen Konstitusi”, *jcl*, vol. 1, no. 3, p. 20, Jul. 2024. <https://doi.org/10.47134/jcl.v1i3.2958>
- [17] E. R. . Wati and A. . Fatah, “Buku Ajar Hukum Pidana”, *umsidapress*, pp. 1–118, Aug. 2021. doi: <https://doi.org/10.21070/2020/978-623-6833-81-0>
- [18] N. Efendi and M. T. Multazam, “Afiliator Liability and Digital Evidence in Binary Option Fraud Prosecution: Tanggung Jawab Afiliator dan Bukti Digital dalam Penuntutan Penipuan Opsi Biner”, *ijler*, vol. 20, no. 4, p. 10.21070/ijler.v20i4.1353, Oct. 2025. doi: <https://doi.org/10.21070/ijler.v20i4.1353>
- [19] C. Agatha and R. Rahaditya, “Fragmented Digital Forensic Standards in Indonesian Criminal Evidence: Standar Digital Forensik yang Terfragmentasi dalam Pembuktian Pidana Indonesia”, *ijler*, vol. 21, no. 2, p. 10.21070/ijler.v21i2.1558, May 2026. doi: <https://doi.org/10.21070/ijler.v21i2.1558>
- [20] I. Efendi dan E. Rosnawati, “Page | 1 Digital Forensic Legal Analysis in Proving Online Sexual Crime Cases Against Children [Analisis Yuridis Digital Forensik dalam Pembuktian Kasus Tindak Pidana Seksual Daring Terhadap Anak].” doi: <https://doi.org/10.21070/ups.8808>

Conflict of Interest Statement:

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.