

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 <i>jo.</i> 51 ayat (1): Manipulasi data agar dianggap otentik. Pasal 27 ayat (1): Distribusi konten melanggar kesusilaan.	<i>Regulatory lag</i> pada AI diatasi dengan delik rekayasa digital (<i>data forgery</i>). Fokusnya membuktikan niat jahat (<i>mens rea</i>) pelaku untuk memalsukan identitas korban.	Menjadi dasar hukum utama untuk menuntut <i>take-down</i> (penghapusan) konten di internet guna memutus 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.

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

NO	Alat Bukti (Pasal 184 KUHAP)	Manifes Teknis / Objek 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 KUHAP)	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 KUHAP)	LHPFD dari Puslabfor Polri.	Diterbitkan secara resmi oleh institusi forensik negara atau ahli independen yang	Keotentikan tanda tangan ahli secara fisik/elektronik.	Celah: Surat dianggap cacat formal jika <i>tools</i> ekstraksi forensik tidak terkalibrasi.

		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.	Surat memuat rincian ilmiah matematis mengenai nilai <i>hash</i> (MD5/SHA-256) berkas video sebelum dan sesudah dianalisis.	Mitigasi: Melampirkan sertifikat kalibrasi perangkat lunak forensik (misal: EnCase/Cellebrite) dalam lampiran berkas perkara.
3.	Petunjuk (Pasal 184 ayat 1 huruf d KUHAP)	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 KUHAP)	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 penyimpanan	Informasi Elektronik dinyatakan sah jika dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan (Pasal 5 & 6 UU ITE). Nilai <i>hash</i> barang bukti konstan dari tahap	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	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. Menghasilkan nilai <i>hash</i> (SHA-256) terhadap berkas arsip web	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]
--	--	--	---	--------------------------------------	--

			tersebut guna mengunci keutuhan data (<i>integrity</i>). [20]		
--	--	--	--	--	--