

ANALISIS YURIDIS PEMBUKTIAN TINDAK PIDANA *DEEFAKE PORN* YANG TERJADI AKIBAT PEMANFAATAN ATAU PENYALAHGUNAAN *ARTIFICIAL INTELLIGENCE (AI)*

Anggraeni; Basrawi; Irabiah; Muhammad As Ari. AM

Email : asariarief01@gmail.com

ABSTRAK

Kecerdasan buatan saat ini disalahgunakan secara besar besaran oleh penjahat dunia maya, *Deepfake* atau Audio/video impersonation (peniruan identitas audio/video) sering digunakan sebagai sarana membuat video manipulasi yang berbau pornografi. Tujuan penelitian ini adalah untuk mengetahui pembuktian tindak pidana penyalahgunaan *Artificial Intelligence (AI) Deepfake Porn* menurut sistem hukum positif di Indonesia. Dan perlindungan hukum bagi korban penyalahgunaan *Artificial Intelligence (AI) Deepfake Porn* menurut sistem hukum positif di Indonesia. Metode penelitian yang digunakan dalam skripsi ini adalah penelitian yuridis normatif, dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Hasil penelitian menunjukkan bahwa menurut Pasal 183 KUHP mensyaratkan minimal dua alat bukti yang sah dan keyakinan hakim untuk memvonis terdakwa. *Deepfake* pornografi sebagai pelanggaran privasi digital menuntut pembuktian melalui forensik digital. Sesuai Pasal 5 ayat (1) dan (2) UU No. 1 Tahun 2024, konten elektronik hasil *Deepfake* sah dijadikan alat bukti dipengadilan. Oleh karena itu, pembuktian atas kepemilikan akun yang digunakan dalam pembuatan maupun penyebaran konten *Deepfake* menjadi sangat penting, karena tanpa hal tersebut, unsur pidana dalam dakwaan tidak dianggap terpenuhi. Dan Perlindungan hukum bagi korban penyalahgunaan teknologi *Artificial Intelligence Deepfake* mencakup: perlindungan hukum preventif, represif (*take down* dan *right to be forgotten*), kompensasi, restitusi, serta penanganan, perlindungan, dan rehabilitasi bagi korban kekerasan seksual.

Kata Kunci: Pembuktian pidana, *Artificial Intelligence (AI)*, *Deepfake Porn*

ABSTRACT

Artificial intelligence is currently being massively misused by cybercriminals. Deepfake or audio/video impersonation is often used as a means to create manipulated videos with pornographic content. The purpose of this research is to understand the legal proof of criminal acts related to the misuse of Artificial Intelligence (AI) Deepfake Porn according to the positive legal system in Indonesia, as well as the legal protection for victims of such misuse under the positive legal system in Indonesia. The research method used in this thesis is normative legal research, employing both a statute approach and a conceptual approach. The research results indicate that according to Article 183 of the Criminal Procedure Code, at least two valid pieces of evidence and the judge's conviction are required to convict the defendant. Deepfake pornography, as a violation of digital privacy, demands proof through digital forensics. According to Article 5 paragraphs (1) and (2) of Law No. 1 of 2024, electronic content resulting from Deepfake is deemed valid evidence in court. Therefore, proving the ownership of the accounts used in the creation and distribution of Deepfake content is very important, because without this, the criminal elements in the indictment are not considered fulfilled. And legal protection for victims of

abuse of Deepfake Artificial Intelligence technology includes: preventive legal protection, repressive measures (take down and right to be forgotten), compensation, restitution, as well as handling, protection, and rehabilitation for victims of sexual violence.

Keywords: Criminal evidence, Artificial Intelligence (AI), Deepfake Porn

PENDAHULUAN

Agar anak dapat tumbuh dengan akhlak yang baik dan mampu bersosialisasi dengan baik untuk memenuhi kebutuhan masa depannya, maka anak harus diperlakukan secara manusiawi. Anak merupakan anugerah dan amanah yang harus dijaga dan dilindungi dengan sungguh-sungguh karena anak memiliki harkat dan martabat yang dijunjung tinggi oleh bangsa. Termasuk di dalamnya adalah pemenuhan kebutuhan jasmani dan rohani. Setiap anak berhak untuk dilindungi dari tindak kekerasan dan diskriminasi serta hak-hak sipil untuk merdeka karena jika dilihat dari perspektif kehidupan berbangsa dan bernegara, anak merupakan pewaris sekaligus cerminan masa depan bangsa, generasi penerus bangsa.¹

AI(Artificial Intelligence) atau kecerdasan buatan merupakan salah satu perkembangan teknologi yang menimbulkan kekhawatiran di banyak negara². Karena kehidupan manusia sangat erat kaitannya dengan teknologi, maka tidak dapat dipungkiri bahwa kejahatan juga berkembang seiring dengan munculnya bentuk bentuk kejahatan baru, seiring dengan banyaknya aspek positif yang ditawarkan dari perkembangan teknologi tersebut. Oleh karena itu, Masyarakat harus mewaspadaai perkembangan teknologi yang berpotensi menjadi sarang kejahatan³

Dari perkembangan teknologi dan informasi ini ditandai dengan munculnya internet sebagai hasil dari penemuan manusia. Internet sendiri merupakan Kumpulan jaringan computer yang saling terhubung yang dapat membaca dan menggunakan berbagai metode komunikasi. Sehingga demikian muncullah jenis kejahatan siber atau cybercrime, merupakan suatu kegiatan melanggar hukum atau kegiatan illegal menggunakan teknologi yang dilakukan melalui jaringan informasi elektronik atau internet. Di Indonesia, kejahatan seksual merupakan salah satu bentuk kejahatan dunia maya yang paling buruk dan menimbulkan kerugian besar bagi masyarakat, terutama Perempuan yang dijadikan objek. Apalagi di era teknologi yang sangat maju ini. Salah satu contoh kejahatan yang sering terjadi adalah penyebaran video pornografi melalui internet atau media social, yang dikenal dengan cyberporn atau pornografi siber.

Tidak dapat dipungkiri bahwa saat ini banyak terjadi kasus Dimana internet

¹ Ihsan Muhammad Anis, 2021. *Pola Pembinaan Anak Yatim Perspektif Hukum Islam dan Undang-Undang Perlindungan Anak: Studi Kasus LKSA di Panti Asuhan Amrillah Kab. Gowa*, Shautuna: Jurnal Ilmiah Mahasiswa Pendidikan Mazhab dan Hukum, Vol. 2, No. 1, hal. 397

² Yusuf, "Perlu Pemahaman Bersama Terkait Pengembangan AI Di Indonesia," Ditjen Aptika Kominfo, 21 Februari 2020, <https://Aptika.Kominfo.Go.Id/2020/02/Perlu-Pemahaman-Bersama-Tentang-Pengembangan-Ai-Di-Indonesia/> Diakses Desember 2024

³ Mansur, Arief & Gultom, "Cyber Law Aspek Hukum Teknologi Informasi", PT Refika Aditama, Bandung :2005, Hlm 9

khususnya media social disalahgunakan sebagai tempat dan sarana penyebaran video porno. Ada banyak kasus Dimana individu membuat video porno dengan memodifikasi wajah serta suara seseorang, ditambah lagi dengan berkembangnya *AI (Artificial Intelligence)* hal tersebut menjadi lebih mudah dilakukan oleh beberapa orang dengan bermodalkan handphone dan kuota internet.

Menurut Widodo, kejahatan dunia maya mengacu pada aktifitas apapun yang dilakukan oleh individu, atau organisasi illegal yang menggunakan computer untuk melakukan kejahatan atau menjadikan computer sebagai target jahat. Semua kejahatan tersebut baik berupa pelanggaran hukum yang berat atau perbuatan yang melanggar ketentuan hukum dalam bentuk apapun⁴.

Kecerdasan buatan mempunyai dampak besar terhadap kehidupan manusia. Namun, kecerdasan buatan saat ini disalahgunakan secara besar besaran oleh penjahat dunia maya, yang disebut dengan kejahatan kecerdasan buatan atau *Artificial Intelligence crime (AIC)*⁵. Salah satu jenis AIC (*Artificial Intelligence crime*) yang dianggap sangat berbahaya dan “mematikan” adalah *Deepfake* atau Audio/video impersonation (peniruan identitas audio/video)⁶. *Deepfake* adalah metode yang banyak digunakan untuk memalsukan atau memanipulasi foto, video dan audio menggunakan Teknik pemindaian menyeluruh dan mendasar terhadap gambar manusia menggunakan teknik *Deep Learning*⁷. *Deepfake* sering digunakan dalam produksi film sebagai hiburan di TV atau sosial media.

Salah satu contoh nyata dari penyalahgunaan *Deepfake* ini yaitu beredarnya video Nagita Slavina yang mengandung unsur pornografi. Diketahui video berdurasi 61 detik tersebut berisikan Nagita Slavina yang merupakan aktris tanah air sedang melakukan Tindakan tak senonoh dan melanggar kesusilaan, tetapi setelah dilaporkan untuk ditindak lanjuti dan diinvestigasi pihak kepolisian menyatakan bahwa video tersebut palsu karena telah direkayasa wajah pemeran dalam video tersebut menggunakan wajah sang aktris yang diambil dari media sosialnya sehingga seolah -olah ia yang berperan dalam video tersebut. Dalam laporan nomor LP/B/100.1/2002/SPKT/ RESORT JAKPUS/PMJ, polisi diminta untuk memproses dan mengusut tuntas mengenai peredaran video tersebut. Sedangkan video tersebut sudah viral dan ada banyak yang mengunggah Kembali sehingga sulit untuk menemukan darimana video tersebut berasal dan siapa yang membuatnya. Kasus video *Deepfake* pornografi milik selebriti tanah air, Nagita Slavina

⁴ Widodo, Prabowo P. Dkk, “*Pemodelan System Berorientasi Obyek Dengan UML*”, (Yogyakarta: Graha Ilmu, 2011), Hlm7.

⁵ Homas C. King, “*Artificial Intelligence Crime: An Interdisciplinary Analysis Of Foreseeable Threats And Solutions*”, Sci Eng Ethics 26 , <https://doi.org/10.1007/S11948-018-00081-0> Diakses 21 Desember 2024.

⁶ M. Caldwell, Dkk. “*AI-Enabled Future Crime*”, Jurnal Crime Scene 9, No. 14 (5 Agustus 2020): 6, <https://doi.org/10.1186/S40163-020-00123-8>

⁷ Muhammad Faqih Fathurrahman Dan Enni Soerjati Priowirjanto, “*Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia*”, Jurnal Indonesia Sosial Teknologi, No. 11 (Desember 2024): 1159, <http://dx.doi.org/10.36418/jist.v3i11.528>

mengalami hambatan dalam pembuktiannya sehingga kasus tersebut ditutup tanpa tindakan hukum lebih lanjut yang diambil oleh pelaku.

Beberapa tahun terakhir, perubahan pada gambar dan video ini lebih banyak memberikan dampak negative dibandingkan positif, khususnya bagi para korban penyebaran konten pornografi, selain itu saat ini ada jenis malware lain yang memanfaatkan algoritme *Deepfake*, seperti seseorang menggunakan video dan suara palsu untuk mencemarkan nama baik dan menipu orang lain, contohnya dalam kasus penipuan yang mengatasnamakan para pejabat pemerintahan seperti MENKEU Sri Mulyani dan Pak Prabowo Subianto. Teknologi buatan ini bertanggung jawab atas kegiatan ilegal dan kejahatan lainnya yang akan terjadi di masa depan dengan kemajuan teknologi yang semakin cepat dan pesat ini.

Pornografi *Deepfake* merupakan kejahatan siber yang semakin canggih dan meresahkan, di mana teknologi kecerdasan buatan digunakan untuk menciptakan konten dewasa palsu yang sangat meyakinkan. Korban, tanpa persetujuan dan sepengetahuan, secara tidak sah digambarkan dalam situasi yang sangat memalukan dan merugikan. Tindakan ini bukan hanya melanggar privasi dan martabat individu, tetapi juga berpotensi menimbulkan dampak psikologis yang sangat mendalam, seperti trauma, depresi, dan kecemasan. Selain itu, korban juga dapat mengalami kerugian materiil akibat pencemaran nama baik dan kesulitan dalam kehidupan sosial. Dalam konteks hukum, pornografi *Deepfake* merupakan pelanggaran terhadap sejumlah ketentuan hukum, termasuk undang-undang tentang pornografi, perlindungan data pribadi, dan tindak pidana.

Negara memiliki kewajiban untuk melindungi warganya dari kejahatan ini melalui penegakan hukum yang tegas dan efektif. Pelaku harus dijerat dengan sanksi pidana yang setimpal untuk memberikan efek jera dan mencegah terjadinya tindak pidana serupa. Selain itu, pemenuhan hak-hak korban, seperti hak untuk mendapatkan perlindungan, pemulihan nama baik, dan dukungan psikologis, juga merupakan bagian integral dari upaya perlindungan korban.

Penyebaran konten *Deepfake* tidak hanya berdampak pada individu, tetapi juga pada masyarakat secara luas. Kepercayaan masyarakat terhadap informasi digital dapat terkikis, dan polarisasi sosial dapat semakin meningkat. Oleh karena itu, pornografi *Deepfake* merupakan ancaman serius terhadap tatanan sosial dan perlu ditangani secara komprehensif.

Deeprtrace pada tahun 2019 dalam surveinya menemukan bahwa, dari hasil rekayasa *Artificial Intelligence Deepfake* adalah konten pornografi sebesar 96%. Setidaknya perusahaan AI (*Artificial Intelligence*) Deeprtrace menemukan sekitar 15.000 video *Deepfake* yang beredar daring pada September tahun 2019, Dan semakin banyak bertambah, bahkan hampir dua kali lipat setiap 10 bulan, dan rata rata yang menjadi

korban adalah perempuan.⁸

Tindak pidana pornografi terdapat pada Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi pada Pasal 4 Ayat (1), yang selanjutnya disebut UU-Pornografi, berbunyi:

“Setiap orang dilarang memproduksi, membuat, memperbanyak, menggandakan, menyebarkan, menyiarkan, mengimpor, mengeksport, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi yang secara eksplisit memuat; persenggamaan, termasuk persenggamaan yang menyimpang; kekerasan seksual; masturbasi atau onani; ketelanjangan atau tampilan yang mengesankan ketelanjangan; alat kelamin; atau pornografi anak”.

Pornografi dalam Kitab Undang-Undang Hukum Pidana (KUHP) ada dalam Pasal 289 KUHP yang menyatakan :

“Barang siapa dengan kekerasan atau ancaman kekerasan memaksa seseorang untuk melakukan atau membiarkan dilakukan perbuatan cabul, diancam karena melakukan perbuatan yang menyerang kehormatan kesusilaan, dengan pidana penjara paling lama sembilan tahun.”

Cyberpornography adalah perbuatan atau kegiatan yang dilakukan dengan membuat, memasang, dan menyebarkan konten yang bermuatan unsur pornografi. Istilah lain untuk ini adalah *cyberpornography* yaitu pendistribusi dan penyebaran konten pornografi ke media internet⁹. Yang termasuk tindak pidana dalam regulasi UU ITE ialah pada pasal 27 ayat (1) UU ITE, berbunyi:

“Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen elektronik yang memiliki muatan yang melanggar kesusilaan.”

Untuk isu pornografi dengan kecanggihan teknologi kecerdasan buatan (*Artificial Intelligence*) terkhususnya teknik *Deepfake* ini juga menjadi suatu permasalahan hangat di kalangan masyarakat sekarang, sehingga sangat dibutuhkan ketentuan yang jelas baik dari segi pembuktian dan perlindungan hukum bagi para korbannya.

Maka dari itu penulis mengambil judul “ Analisis Yuridis Pembuktian Tindak Pidana *Deepfake Porn* Yang Terjadi Akibat Pemanfaatan Atau Penyalahgunaan *Artificial Intelligence (AI)*”.

METODE PENELITIAN

Peneliti menggunakan metode penelitian dengan penerapan kajian hukum normatif. Penelitian hukum normatif adalah penelitian yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagai bahan dasar untuk diteliti dengan cara

⁸ Deeptrace, “The State Of *Deepfakes*: Landscape, Threats And Impact”, 29 Desember 2024, [Http://Deeptracelabs.Com/Reports/](http://Deeptracelabs.Com/Reports/).

⁹ Mahsun Ismail, “Kebijakan Hukum Pidana Cyberpornography Terhadap Perlindungan Korban”, Vol. 1, No. 2, Jurnal Hukum Ekonomi Syariah , Hlm. 119.

mengadakan penelusuran terhadap peraturan-peraturan dan literatur-literatur yang berkaitan dengan permasalahan yang diteliti.

Penulis menggunakan metode pendekatan peraturan perundang undangan dan pendekatan konseptual sebagai bahan utama dalam proses penelitian. Pendekatan ini merupakan penelitian yang mengutamakan bahan hukum yang berupa peraturan perundang-undangan sebagai bahan acuan dasar dalam melakukan penelitian dan pendekatan yang beranjak dari pandangan dan doktrin yang berkembang di dalam ilmu hukum.

Analisis data hukum akan dilakukan dengan cara deskriptif dan kualitatif, yang berarti bahwa data data yang sebenarnya kemudian dikumpulkan, diproses dan dianalisis untuk menggambarkan tentang masalah yang sedang diteliti. Teknik analisis data deskriptif kualitatif adalah teknik analisis data yang bertujuan untuk mendeskripsikan atau memberikan gambaran terhadap fenomena atau kejadian yang sedang diteliti.

HASIL DAN PEMBAHASAN

1. Pembuktian Tindak Pidana Penyalahgunaan *Artificial Intelligence (AI) Deepfake Porn* Menurut Sistem Hukum Positif Di Indonesia

Salah satu prinsip utama sistem pembuktian di Indonesia adalah minimum bewijs, atau pembuktian minimal, yang diatur dalam Pasal 183 KUHAP, yang mensyaratkan bahwa seorang terdakwa hanya dapat dinyatakan bersalah jika ada sekurang-kurangnya dua alat bukti yang sah, ditambah keyakinan hakim. Alat bukti ini dapat berupa keterangan saksi, keterangan ahli, dokumen, petunjuk, atau keterangan terdakwa, sebagaimana diatur dalam Pasal 184 KUHAP.

Pembuktian secara sah menurut undang-undang adalah prinsip kedua yang mendasari sistem pembuktian di Indonesia. Ini berarti bahwa bukti yang diajukan harus memenuhi persyaratan hukum, baik dalam hal pengumpulan, penyampaian, maupun keabsahannya. Prinsip ini menekankan pentingnya prosedur yang sesuai hukum dalam setiap tahap pengumpulan bukti untuk melindungi hak asasi manusia dan memastikan keadilan dalam proses peradilan.

Prinsip lainnya adalah pembebanan beban pembuktian yang sebagian besar berada di pihak penuntut umum. Dalam sistem hukum pidana Indonesia, jaksa sebagai penuntut umum memiliki kewajiban untuk membuktikan bahwa terdakwa bersalah atas tindak pidana yang didakwakan.¹⁰

Manipulasi terhadap konten visual dan audio kini telah mencapai tingkat kecanggihan yang memungkinkan penciptaan media digital yang tampak sangat nyata, padahal sebenarnya sepenuhnya hasil rekayasa. Bentuk manipulasi ini, yang dikenal sebagai *Deepfake*, melibatkan penggunaan teknologi kecerdasan buatan khususnya

¹⁰ M.Hatta Z. Husni, "Kejahatan Penistaan Agama Dan Konsekuensi Hukumnya " Jurnal Hukum Vol 13 No 2, 2021

algoritma pembelajaran mesin seperti *deep learning* dan *generative adversarial networks (GANs)* untuk mengganti wajah, ekspresi, atau suara seseorang dengan individu lain. Hasil akhirnya adalah video, gambar, atau rekaman suara yang memperlihatkan seseorang seolah-olah sedang melakukan tindakan atau mengucapkan pernyataan tertentu, padahal dalam kenyataannya hal tersebut tidak pernah terjadi.¹¹

Perkembangan teknologi *Deepfake* dalam era *AI* telah membawa dampak signifikan di berbagai bidang. Dalam industri film, *Deepfake* digunakan untuk meningkatkan produksi efek visual (VFX), memungkinkan penciptaan adegan yang lebih realistis dan kreatif.¹² Namun, kemudahan pembuatan *Deepfake* juga menimbulkan ancaman terhadap privasi dan keamanan, karena dapat digunakan untuk menciptakan berita palsu atau merusak reputasi individu dengan manipulasi konten ke berbau pornografi.¹³

Dari sudut pandang penegakan hukum, *AI* telah menjadi alat bantu yang sangat berharga bagi aparat, terutama dalam meningkatkan efektivitas investigasi, mempercepat proses analisis data, dan membantu mengidentifikasi pola-pola tindak pidana yang sulit terlihat oleh pengamatan manusia biasa. Misalnya, sistem *AI* dapat digunakan untuk menganalisis rekaman *CCTV* secara otomatis guna mengenali wajah pelaku kejahatan, membaca plat nomor kendaraan dalam waktu nyata, atau menghubungkan berbagai informasi dari database kriminal untuk memetakan jaringan kejahatan. Bahkan, dalam konteks pencegahan, *AI* juga digunakan untuk memprediksi potensi lokasi atau waktu terjadinya tindak pidana berdasarkan tren historis dan faktor-faktor risiko tertentu, sebuah pendekatan yang dikenal sebagai *predictive policing*.¹⁴

Sebagai bagian penting dari suatu persidangan pidana, pembuktian merupakan langkah penting dalam penyelesaian suatu perkara pidana. Sebagaimana dijelaskan oleh Eddy Hiariej, fungsi penting alat bukti pidana berkaitan dengan pencarian kebenaran dalam suatu perkara hukum, yang berarti bahwa kejahatan mencari kebenaran nyata atau fakta.¹⁵ Cybercrime dapat didefinisikan sebagai kejahatan yang menggunakan fasilitas internet, dan karena itu memerlukan metode khusus untuk menemukan dan mengumpulkan barang bukti agar dakwaan dapat dibuktikan.¹⁶

¹¹ Muh. Taufik Darmawan, Amir Junaidi, Ariy Khaerudin, "Penegakan Hukum Terhadap Penyalahgunaan *Deepfake* Pada Pornografi Anak Di Era Artificial Intelligence Di Indonesia" Jurnal Serambi Hukum Vol 18 No 01 Tahun 2025, Hlm 47.

¹²Hardeep Singh Et Al., "Deepfake As An Artificial Intelligence Tool For VFX Films," 2023 7th International Conference On Computation System And Information Technology For Sustainable Solutions (CSITSS), 2023, 1–5, <https://doi.org/10.1109/CSITSS60515.2023.10334186>.

¹³ Jayanta Kumar Panda And Rajnandini Panigrahy, "Unmasking Deception In The Age Of Artificial Intelligence: A Comprehensive Analysis Of Indian Celebrity's Deepfakes News," Shodhkosh:Journalofvisualandperformingarts,2023,<https://doi.org/10.29121/Shodhkosh.V4.I2>.

¹⁴ Tzu-Wei Hung And Chun-Ping Yen, "On The Person-Based Predictive Policing Of AI," Ethics And Information Technology 23 (2025): 165–76, <https://doi.org/10.1007/S10676-020-09539-X>.

¹⁵ . Eddy O. S. Hariariej, Teori Dan Hukum Pembuktian, (Jakarta: Penerbit Erlangga, 2022),Hlm 7

¹⁶ Budi Kristian Bivanda Putra, Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) Di Indonesia, Pamulang Law Review Vol.1 No.1, Agustus 2018, Hlm. 6

Proses mengambil, memulihkan, menyimpan, atau memeriksa dokumen atau informasi elektronik dalam sistem elektronik atau media penyimpanan dengan alat dan metode ilmiah yang membantu proses pembuktian dikenal sebagai forensik digital¹⁷

Forensik digital diperlukan dalam pembuktian *Deepfake porn* yang terjadi di media sosial, karena kejahatan tersebut terjadi di media elektronik, sehingga akan diperoleh informasi elektronik dan/atau dokumen elektronik. Berdasarkan apa yang tertuang dalam Putusan Mahkamah Konstitusi No. 20/PUU XIV/2016, atas permintaan aparat penegak hukum, informasi elektronik dan/atau dokumen elektronik dapat digunakan sebagai alat bukti di persidangan.

Informasi dan/atau dokumen elektronik berupa foto atau gambar sebagaimana diatur dalam Pasal 5 ayat (1) dan (2) UU 1/2024 adalah alat bukti hukum yang sah. barang bukti elektronik sifatnya tidak terlihat, rapuh, peka terhadap waktu, mudah dirusak, mudah direkayasa, dan mudah dimusnahkan.¹⁸

pentingnya membuktikan kepemilikan akun dalam proses pembuatan dan penyebaran konten *Deepfake porn* dengan forensik digital yakni bahwa memaksakan tanggung jawab pada seseorang dalam hukum pidana berarti tidak hanya seseorang itu secara yakin dan sah terbukti melakukan kejahatan, tetapi juga memiliki keyakinan penuh bahwa itu benar untuk menjatuhkan persangkaan kepadanya dan meminta pertanggungjawabannya. jika tidak dapat dibuktikan apakah subjek hukum yang dihadirkan di muka persidangan adalah pemilik akun yang membuat dan konten *Deepfake porn*, maka unsur pasal yang didakwa kepadanya dianggap tidak terpenuhi.¹⁹

Melakukan forensik digital harus didasarkan pada beberapa prinsip dasar agar analisis bukti dapat dijamin keasliannya dan diterima dalam proses persidangan. Prinsip-prinsip ini termasuk prinsip Dokumentasi atau *chain of custody*, kompetensi, bertanggung jawab, dan diuji dan disajikan²⁰.

4 (empat) tahap yang akan dilakukan dalam pemeriksaan digital forensik untuk memeriksa barang bukti yang diperoleh dari suatu tindak pidana siber²¹

1. Identifikasi Bukti, Proses forensik digital yang paling penting adalah identifikasi barang bukti. Ini mencakup identifikasi lokasi barang bukti, tempat penyimpanan, dan metode penyimpanan, sehingga data yang disimpan dalam barang bukti memiliki karakteristik yang sama dan tidak dapat diubah.

¹⁷ Agung Purnama Saputra, Analisis Digital Forensik Pada File Steganography, Jurnal Teknik Informatika Dan Sistem Informasi Vol.2 No.1, April 2022. Hlm.180

¹⁸ Eddy Army, Op.Cit, Hlm.141

¹⁹ Huda Chairul, Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan, Jakarta, 2022, Hlm.64

²⁰ Muhammad Nuh Al-Azhar, Digital Forensic Panduan Praktis Investigasi Komputer, (Jakarta: Salemba Infotek, 2021), hlm.3

²¹ Asrizal, Digital Forensik-Apa dan Bagaimana,

<http://edokumen.kemenag.go.id/files/VQ2Hv7uT1339506324.pdf>, Pada 1 JULI 2025

2. Analisis Bukti: Pada tahap ini, bukti yang telah dikumpulkan diperiksa kembali dalam konteks investigasi yang relevan, termasuk memeriksa metadata. Faktor-faktor seperti jumlah sesi pengeditan, nama komputer, berapa kali file disimpan, lokasi file dicetak, dan tanggal dan waktu perubahan dimasukkan ke dalam file. Pada langkah berikutnya, juga dilakukan proses pemulihan seperti pemulihan kata sandi, file dan folder yang dihapus, membuat ulang partisi, membuka format drive, membangun kembali halaman web yang dikunjungi, pemulihan email yang dihapus, dan sebagainya.
3. Presentasi, Tahap presentasi adalah tahap di mana bukti yang ada divalidasi dan hubungannya dengan kasus yang ada.

Teknik forensik digital sangat bervariasi tergantung pada jenis bukti yang sedang dianalisis dan perangkat yang digunakan ²². Forensik digital dapat digunakan untuk menemukan bukti yang mendukung argumen salah satu pihak. Yakni dengan memulihkan email yang dihapus, dokumen penting, atau log aktivitas digital yang menunjukkan siapa yang melakukan manipulasi foto atau video menggunakan aplikasi pendukung.

Sehingga dalam hal membuktikan tersangka pelaku *Deepfake* porn ini bisa dibuktikan dengan menggunakan digital forensik walaupun pelaku sudah menghapus *history* ataupun menggunakan *anomitas*. tetapi dalam hal ini banyak model digital forensik yang ada saat ini dilatih untuk mengenali jenis *Deepfake* tertentu, sehingga kesulitan dalam mendeteksi *Deepfake* yang dihasilkan dengan teknik yang berbeda. ²³

Sudah ada banyak pelaku kasus *Deepfake* porn yang telah ditangkap dengan cara patroli siber rutin yang dilakukan jajaran Polres setiap daerah awal Juni 2025, tim siber menemukan banyak akun mencurigakan yang menawarkan jasa pembuatan video porno dengan fitur penggantian wajah menggunakan teknologi *Deepfake*. Layanan tersebut bahkan menerima pesanan dari publik, asalkan menyertakan foto wajah target yang ingin dipasang dalam video. ²⁴

Kasus tersebut tergolong sebagai *Deepfake* sederhana. Adapun *Deepfake* yang menggunakan *AI* sebagai perisai memiliki kemampuan untuk mengaburkan identitas pelaku, memanipulasi *metadata*, dan menyamarkan aktivitas digital sedemikian rupa sehingga pelacakan hampir mustahil dilakukan tanpa alat forensik digital yang sangat maju dalam kata lain Pelaku kejahatan memanfaatkan berbagai teknologi untuk menyembunyikan komunikasi dan bukti yang tersimpan di komputer dari pihak berwenang. Contoh *Deepfake* yang menggunakan *ransomware AI* dimana digunakan

²² Nita Azhar "Tahapan Dan Teknik Forensik Digital Dalam Mengungkap Kejahatan Dunia Maya" IDS Digital College <https://ids.ac.id/tahapan-dan-teknik-forensik-digital-dalam-dunia-maya/>

²³ D Coccomini, "Deepfake Detection: Challenges And <https://consensus.app/papers/deepfake-detection-challenges-and-solutions-coccomini/E1b9d4babc1f50799ba4247904e10509/>.

²⁴ Zaky Al-Yamani Fakta Mengejutkan Di Balik Kasus Video Porno Berteknologi *Deepfake* Yang Diungkap Polres Kendal <https://www.viva.co.id/trending/1829272-5-fakta-mengejutkan-di-balik-kasus-video-porno-berteknologi-deepfake-yang-diungkap-polres-kendal>.

untuk mengotomatisasi serangan, menyembunyikan diri dari sistem keamanan, dan mengevaluasi sistem target secara lebih cerdas sebelum menyerang. Sehingga dalam hal ini menjadi hambatan dalam proses forensik digital.

Perbedaan antara proses digital forensik pembuktian kasus *deepfake porn* dengan kasus yang lain yakni proses mencari apakah konten tersebut hasil rekayasa atau tidak dengan memerlukan analisis multimedia forensik, termasuk deteksi artefak pada wajah (*blink rate*, pergerakan bibir tidak sinkron), analisis *metadata* untuk jejak manipulasi, penggunaan *AI-based detection tools* seperti Microsoft Video Authenticator dan Deepware Scanner.²⁵ Kasus Lain seperti Peretasan, Penyebaran Malware, dll. lebih berfokus Fokus pada log aktivitas digital, file konfigurasi, alamat IP, jejak digital pengguna, komunikasi email, atau keberadaan malware. Contohnya seperti analisis network traffic, registry entries, dan file log sistem²⁶.

2. Perlindungan Hukum Bagi Korban Penyalahgunaan Artificial Intelligence (AI) Deepfake Porn Menurut Sistem Hukum Positif Di Indonesia

Perlindungan hukum merupakan salah satu wujud nyata dari fungsi negara dalam menjamin dan mengawal pelaksanaan hak asasi manusia bagi setiap warga negara, tanpa terkecuali²⁷.

Hak asasi manusia adalah hak fundamental yang melekat pada setiap individu sejak lahir dan tidak dapat dicabut oleh siapa pun. Negara, melalui lembaga dan perangkat hukumnya, berkewajiban melindungi hak-hak tersebut dari berbagai bentuk ancaman, pelanggaran, atau penyalahgunaan oleh pihak lain, baik yang berasal dari individu, kelompok, maupun institusi.²⁸

Dalam konteks ini, perlindungan hukum memiliki arti penting sebagai mekanisme formal dan institusional yang bertujuan untuk memberikan rasa aman, menjamin keadilan, serta mencegah terjadinya praktik-praktik sewenang-wenang yang dapat merugikan masyarakat. Perlindungan hukum bukan hanya sekadar bentuk reaksi terhadap tindakan melanggar hukum, tetapi juga mencakup langkah-langkah preventif yang dirancang untuk meminimalkan kemungkinan terjadinya pelanggaran.

Bentuk perlindungan hukum untuk korban yang dapat diterapkan untuk korban penyalahgunaan *Artificial Intelligence Deepfake*, yaitu:

1. Perlindungan Hukum Preventif: Undang-undang yang berkaitan dengan penyalahgunaan kecerdasan buatan *Deepfake*, atau UU-ITE, serta undang-undang khusus lain yang berkaitan

²⁵ Anggraini, T. "Analisis Forensik Digital terhadap Bukti Deepfake dalam Penegakan Hukum Siber di Indonesia", 2020 *Jurnal Hukum & Teknologi*, Vol. 6 No. 2

²⁶ Nelson, B., Phillips, A., & Steuart, C. "Guide to Computer Forensics and Investigations", 2020, Cengage Learning. Hlm 153-180

²⁷ Topo Santoso, Hukum Pidana: Suatu Pengantar, 1 (Depok: Rajawali Pers, 2021). (Depok: Rajawali Pers, 2021). Hlm 19

²⁸ Kansil, Pengantar Ilmu Hukum Dan Tata Hukum Indonesia (Jakarta: Balai Pustaka, 2018). (Jakarta: Balai Pustaka, 2018). 76

dengan tindak pidana yang dilakukan oleh pelaku memberikan perlindungan hukum preventif.

2. Perlindungan represif adalah langkah terakhir yang dapat diambil korban untuk dilindungi dari konflik atau pelanggaran yang dilakukan oleh pelaku. Denda, hukuman penjara, dan bentuk hukuman lainnya adalah bentuk perlindungan represif.
3. Penanganan, Perlindungan, dan Rehabilitasi Bagi Korban Kekerasan Seksual.

Pasal 4 Ayat (1) UU-TPKS membahas berbagai jenis kekerasan seksual, termasuk pelecehan seksual nonfisik dan seksual; pelecehan seksual fisik; pemaksaan kontrasepsi, pemaksaan sterilisasi, pemaksaan perkawinan; penyiksaan seksual; eksploitasi seksual; perbudakan seksual; dan kekerasan seksual berbasis elektronik. Penyalahgunaan pornografi Deepfake, yang merupakan contoh penyalahgunaan teknologi kecerdasan buatan, termasuk tindak pidana kekerasan seksual berbasis elektronik, yang dapat berupa memulai penyebaran konten pribadi melalui media online dan sosial, seperti gambar, video, dan dokumen elektronik lainnya yang mengandung konten seksual di luar kehendak korban. Oleh karena itu, korban dalam kasus ini berhak atas hak-hak yang dilindungi oleh UU TPKS, yang mencakup hak penanganan, perlindungan, dan pemulihan atau rehabilitasi. Hak penanganan meliputi hak untuk mendapatkan informasi tentang seluruh proses dan hasil penanganan, perlindungan, dan pemulihan.

Hak penanganan termasuk hak atas informasi tentang proses penanganan, perlindungan, dan pemulihan; hak atas dokumen hasil penanganan; hak atas layanan hukum; hak atas bantuan psikologis; hak atas pemeriksaan medis, tindakan, dan perawatan; hak atas layanan dan fasilitas yang sesuai dengan kebutuhan khusus Korban; dan hak atas penghapusan konten bermuatan seksual dalam kasus kekerasan seksual di media elektronik.

Hak perlindungan mencakup perlindungan korban dari ancaman atau kekerasan dari pelaku atau pihak lain, serta kekerasan berulang; perlindungan identitas pribadi; perlindungan dari sikap dan perilaku penegak hukum yang merendahkan korban; perlindungan dari kehilangan pekerjaan, mutasi pekerjaan, akses politik, atau pendidikan; dan perlindungan dari kehilangan pekerjaan, pendidikan, atau akses politik.²⁹

Hak pemulihan atau rehabilitasi berupa: Rehabilitasi medis; Rehabilitasi mental dan sosial; pemberdayaan sosial; Restitusi dan/atau kompensasi; dan reintegrasi sosial³⁰.

4. Hak Untuk Dilupakan (*Right To Be Forgotten*)

Hak untuk dilupakan, atau hak untuk dilupakan, diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Dokumen Elektronik, yang menyatakan: "Setiap Penyelenggara Sistem Elektronik wajib menghapus

²⁹ Pasal 69 Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual

³⁰ Pasal 70 Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual

Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan Orang yang bersangkutan berdasarkan penetapan pengadilan."

Pengertian dari penghapusan (*right to erasure*) sesuai dengan pasal 15 Ayat (1) PP-PSTE berarti kewajiban untuk menghapus informasi elektronik dan/atau dokumen elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan. Sedangkan pengertian pengeluaran dari daftar mesin pencari tertera dalam penjelasan Pasal 15 Ayat (2) PP-PSTE adalah kewajiban mengeluarkan dari daftar mesin pencari meliputi Penyelenggara Sistem Elektronik yang menjalankan mesin pencari untuk menghapus penampilan dan/ atau menutup Akses terhadap Informasi Elektronik dan/ atau Dokumen elektronik yang tidak relevan tersebut berdasarkan penetapan pengadilan.

5. Tindakan Pemutusan Akses (*Take Down*)

Menurut Pasal 1 Angka 15 Peraturan Menteri Komunikasi dan Informatika Nomor 10 Tahun 2021 Tentang Perubahan Atas Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat, yang selanjutnya disebut PERMENKOMINFO-PSE, pemutusan akses (*take down*) didefinisikan sebagai penutupan akses, penutupan akun, dan/atau yang terintegrasi. Pasal 13 PERMENKOMINFO-PSE menyatakan bahwa "PSE Lingkup Privat wajib melakukan Pemutusan Akses (*take down*) terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud dalam Pasal 9 ayat (4)."

Menurut Pasal 9 Ayat (4) PERMENKOMINFO-PSE, *takedown* dapat dilakukan terhadap informasi dan dokumen elektronik yang melanggar undang-undang, meresahkan masyarakat, atau mengganggu ketertiban umum. *Takedown* juga dapat dilakukan terhadap informasi dan dokumen elektronik yang memfasilitasi penyebaran informasi. Ada kemungkinan bahwa masyarakat, kementerian atau lembaga, aparat penegak hukum, dan/atau lembaga peradilan meminta tindakan *take down*. Anda dapat mengajukan permohonan melalui aplikasi online, surat non elektronik, atau e-mail.³¹

6. Kompensasi

Menurut Pasal 1 Angka 10 dari Undang-Undang Nomor 31 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi dan Korban (UU-PSK), kompensasi adalah: "Ganti kerugian yang diberikan oleh negara karena pelaku tidak mampu memberikan ganti kerugian sepenuhnya yang menjadi tanggung jawabnya kepada Korban atau Keluarganya".

Dalam Pasal 7 UU-PSK, berbunyi: "Setiap Korban pelanggaran hak asasi manusia

³¹ Pasal 14 Ayat (2) Peraturan Menteri Komunikasi Dan Informatika Nomor 10 Tahun 2021 Tentang Perubahan Atas Peraturan Menteri Komunikasi Dan Informatika Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat

yang berat dan Korban tindak pidana terorisme selain mendapatkan hak sebagaimana dimaksud dalam Pasal 5 dan Pasal 6, juga berhak atas Kompensasi”.

hanya korban atas pelanggaran Hak Asasi Manusia berat seperti tindak pidana terorisme, perdagangan orang, penyiksaan, kekerasan seksual, dan korban penganiyaan berat yang dapat mengajukan kompensasi. Kompensasi diajukan oleh korban, keluarga, atau kuasanya melalui LPSK (Lembaga Perlindungan Saksi dan Korban) kemudian diajukan ke muka pengadilan.³²

7. Restitusi

Dalam UU-PPK Pasal 1 Angka 11, restitusi yaitu ganti kerugian yang diberikan kepada korban atau keluarganya oleh pelaku atau pihak ketiga. Pasal 7A UU-PPK, korban kekerasan seksual berhak memperoleh restitusi berupa; ganti kerugian atas kehilangan kekayaan atau penghasilan; ganti kerugian yang ditimbulkan akibat penderitaan yang berkaitan langsung sebagai akibat tindak pidana; dan/atau penggantian biaya perawatan medis dan/atau psikologis.

Restitusi juga dijelaskan dalam Pasal 30 Ayat (2) UUP-PPK yang berupa; Ganti kerugian atas kehilangan kekayaan atau penghasilan; Ganti kerugian yang ditimbulkan akibat penderitaan yang berkaitan langsung sebagai akibat tindak pidana kekerasan seksual; Penggantian biaya perawatan medis dan/ atau psikologis; dan/ atau Ganti kerugian atas kerugian lain yang diderita korban sebagai akibat tindak pidana kekerasan seksual. Jika pelaku PPK adalah anak, maka pemberian restitusi diberikan oleh orang tua atau wali dari pelaku.³³

Pada tahun 2018, *Google* melakukan langkah signifikan dengan menambahkan fitur yang secara khusus ditujukan untuk mendeteksi dan menghapus "*citra foto pornografi yang tidak sengaja*" dalam hasil penelusuran mereka. Fitur ini memungkinkan *Google* untuk secara otomatis memasukkan jenis konten tersebut ke dalam daftar hitam atau *ban list*, yang berfungsi sebagai filter untuk mencegah penyebaran materi yang melanggar ketentuan. Selain itu, *Google* juga menyediakan mekanisme bagi penggunanya untuk melaporkan temuan konten yang berisi informasi palsu atau misinformasi, sehingga meningkatkan partisipasi aktif dalam menjaga kualitas informasi yang beredar di platform mereka. Fitur pelaporan ini juga memungkinkan masyarakat untuk berperan serta dalam memerangi penyebaran konten berbahaya atau menyesatkan, memberikan pendekatan yang lebih transparan dalam pengelolaan konten yang dapat diakses oleh pengguna.

Meskipun langkah yang diambil oleh *Google* ini patut dihargai dan menjadi contoh positif dalam hal penanggulangan penyebaran konten pornografi dan informasi palsu, kenyataannya masih terdapat banyak platform digital lain yang belum memiliki regulasi atau fitur serupa untuk mengatasi masalah yang semakin serius ini. Tidak semua penyedia layanan digital menerapkan kebijakan yang cukup ketat dalam hal pengendalian konten

³² Pasal 7 Ayat (2) Undang-Undang Nomor 31 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi Dan Korban

³³ Pasal 37 Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual

berbahaya, termasuk *Deepfake* pornografi yang semakin sering ditemui di berbagai situs. Konten manipulatif semacam ini, yang dapat mengancam privasi individu dan menyebarkan kebohongan atau propaganda, masih dapat tersebar luas di platform-platform yang tidak memiliki sistem deteksi atau pelaporan yang memadai. Hal ini menunjukkan adanya celah regulasi yang besar, yang memungkinkan penyebaran materi ilegal dan merugikan untuk terus berkembang tanpa kontrol yang cukup.

Karena itu, meskipun *Google* telah menunjukkan upaya proaktif dalam mengatasi masalah ini, masih banyak tantangan yang harus dihadapi di tingkat global, terutama dalam hal pengaturan dan implementasi kebijakan yang lebih ketat di platform lain. Peran pemerintah, lembaga pengatur, dan penyedia layanan digital sangat penting untuk memperkuat regulasi dan menciptakan standar global yang seragam dalam menangani masalah konten manipulatif, termasuk *Deepfake*. Hal ini akan memerlukan kolaborasi yang lebih besar antara sektor publik dan swasta, serta komitmen untuk membangun sistem yang lebih efektif dalam menjaga ruang digital tetap aman dan bebas dari eksploitasi.³⁴

PENUTUP

Simpulan

1. Dalam hukum pidana Indonesia, Pasal 183 KUHP mensyaratkan minimal dua alat bukti yang sah dan keyakinan hakim untuk memvonis terdakwa. *Deepfake* pornografi sebagai pelanggaran privasi digital menuntut pembuktian melalui forensik digital. Sesuai Pasal 5 ayat (1) dan (2) UU No. 1 Tahun 2024, konten elektronik hasil *Deepfake* sah dijadikan alat bukti dipengadilan. Oleh karena itu, pembuktian atas kepemilikan akun yang digunakan dalam pembuatan maupun penyebaran konten *Deepfake* menjadi sangat penting, karena tanpa hal tersebut, unsur pidana dalam dakwaan tidak dianggap terpenuhi. Sangat bermanfaat bagi perkembangan kemampuan mental, fisik, dan seni anak asuh apabila hak-hak mereka untuk mendapatkan pendidikan terpenuhi, termasuk apabila panti asuhan anak asuh memberikan layanan pembinaan. Setiap anak asuh berhak untuk mendapatkan layanan pendidikan, baik pendidikan formal maupun informal, berkat pembinaan yang diberikan oleh panti asuhan anak asuh.
2. Perlindungan hukum bagi korban penyalahgunaan teknologi *Artificial Intelligence Deepfake* mencakup: perlindungan hukum preventif, represif (*take down* dan *right to be forgotten*), kompensasi, restitusi, serta penanganan, perlindungan, dan rehabilitasi bagi korban kekerasan seksual.

³⁴ Faqih Dan Soerjati Priowirjanto, "Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan *Deepfakes* Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia.", *Jurnal Indonesia Sosial Teknologi*, Vol. 3, No. 11. 79

Saran

1. Untuk mengatasi tantangan dari perspektif teknis, hukum, dan etika, diperlukan reformasi menyeluruh dalam sistem pembuktian hukum pidana di Indonesia. Ini termasuk pembaruan regulasi, seperti revisi KUHAP untuk mengakomodasi bukti modern, serta pelatihan berkelanjutan bagi aparat hukum untuk meningkatkan kompetensinya. Selain itu, penegakan etika dalam pengumpulan bukti harus diprioritaskan melalui pengawasan ketat dan sanksi terhadap pelanggaran. Dengan langkah-langkah ini, diharapkan tantangan dalam proses pembuktian dapat diminimalkan, sehingga keadilan dalam proses peradilan dapat ditegakkan secara lebih efektif.
2. Penulis menyarankan beberapa langkah penting yang bisa dilakukan untuk menangani masalah penyalahgunaan teknologi *Deepfake*, khususnya yang berkaitan dengan konten pornografi. Salah satunya adalah memperkuat perlindungan dan penegakan hukum, baik sebelum kejahatan terjadi (preventif) maupun setelahnya (represif). Pemerintah punya peran besar dalam hal ini, misalnya dengan membuat undang-undang khusus yang mengatur penggunaan kecerdasan buatan. Tak hanya soal hukum, perhatian juga perlu diberikan pada korban, terutama mereka yang mengalami kekerasan seksual di dunia digital. Dukungan hukum dan psikologis sangat penting bagi proses pemulihan mereka. Langkah pencegahan lainnya bisa berupa edukasi kepada masyarakat tentang bahaya dan potensi penyalahgunaan *AI*. Karena kejahatan semacam ini bisa terjadi lintas negara, kerja sama internasional juga dibutuhkan agar penanganannya lebih efektif. Selain itu, platform digital seperti media sosial dan penyedia konten visual perlu memiliki aturan yang ketat soal penyebaran konten palsu. Sering kali, pelaku mengambil foto pribadi dari media sosial untuk kemudian dimanipulasi menjadi konten *Deepfake* yang merugikan. Karena itu, perlindungan data pribadi dan pengawasan konten sangat penting untuk mencegah hal-hal semacam ini terjadi.

DAFTAR PUSTAKA

- Agung Purnama Saputra, Analisis Digital Forensik Pada File Steganography, Jurnal Teknik Informatika Dan Sistem Informasi Vol.2 No.1, April 2022.
- Anggraini, T. "*Analisis Forensik Digital terhadap Bukti Deepfake dalam Penegakan Hukum Siber di Indonesia*", 2020 *Jurnal Hukum & Teknologi*, Vol. 6 No. 2
- Asrizal, Digital Forensik Apa dan Bagaimana, <http://edokumen.kemenag.go.id/files/VQ2Hv7uT1339506324.pdf>, Pada 1 JULI 2025
- Budi Kristian Bivanda Putra, Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) Di Indonesia, *Pamulang Law Review* Vol.1 No.1, Agustus 2018,

- Dcocomini “*Deepfake* Detection: Challeng And
<https://Consensus.App/Papers/Deepfake-Detection-Challenges-And-Solutions-Cocomini/E1b9d4babcf50799ba4247904e10509/>.
- Deeprace, “The State Of *Deepfakes*: Landscape, Threats And Impact”, 29 Desember 2024, <http://Deepracelabs.Com/Reports/>.
- Eddy O. S. Hariariej, *Teori Dan Hukum Pembuktian*, (Jakarta: Penerbit Erlangga, 2022)
- Euggelia C.P Rumetor, Rony Sepang, Dan Nurhikmah Nachrawy, “Perlindungan Hukum Terhadap Korban Kekerasan Seksual Berbasis Elektronik Menurut Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual”, *Lex Privatum* 11, No. 5 (30 Juni 2023):
- Faqih Dan Soerjati Priowirjanto, “Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan *Deepfakes* Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia.”, *Jurnal Indonesia Sosial Teknologi*, Vol. 3, No. 11.
- Hardeep Singh Et Al., “*Deepfake* As An Artificial Intelligence Tool For VFX Films,” 2023 7th International Conference On Computation System And Information Technology For Sustainable Solutions (CSITSS), 2023, 1–5, <https://doi.org/10.1109/CSITSS60515.2023.10334186>.
- Huda Chairul, *Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan*, Jakarta, 2022,
- Ihsan Muhammad Anis, 2021. *Pola Pembinaan Anak Yatim Perspektif Hukum Islam dan Undang-Undang Perlindungan Anak: Studi Kasus LKSA di Panti Asuhan Amrillah Kab. Gowa*, Shautuna: Jurnal Ilmiah Mahasiswa Pendidikan Mazhab dan Hukum, Vol. 2, No. 1.
- Jayanta Kumar Panda And Rajnandini Panigrahy, “Unmasking Deception In The Age Of Artificial Intelligence: A Comprehensive Analysis Of Indian Celebrity’s *Deepfakes* News,”
 Shodhkosh:Journalofvisualandperformingarts,2023,<https://doi.org/10.29121/Shodhkosh.V4.I2>.
- Kansil, *Pengantar Ilmu Hukum Dan Tata Hukum Indonesia* (Jakarta: Balai Pustaka, 2018). (Jakarta: Balai Pustaka, 2018).
- M. Caldwell, Dkk. “*AI-Enabled Future Crime*”, *Jurnal Crime Scene* 9, No. 14 (5 Agustus 2020): 6, <https://doi.org/10.1186/S40163-020-00123-8>
- M.Hatta Z. Husni,” *Kejahatan Penistaan Agama Dan Konsekuensi Hukumnya* “ *Jurnal Hukum* Vol 13 No 2,2021
- Mahsun Ismail, “Kebijakan Hukum Pidana Cyberpornography Terhadap Perlindungan Korban”, Vol. 1, No. 2, *Jurnal Hukum Ekonomi Syariah*.
- Muh. Taufik Darmawan, Amir Junaidi, Ariy Khaerudin,” *Penegakan Hukum Terhadap Penyalahgunaan Deepfake Pada Pornografi Anak Di Era Artificial Intelligence Di Indonesia*” *Jurnal Serambi Hukum* Vol 18 No 01 Tahun 2025,
- Muhammad Faqih Fathurrahman Dan Enni Soerjati Priowirjanto, “Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan *Deepfakes* Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia”, *Jurnal Indonesia Sosial Teknologi*, No. 11 (Desember 2024): 1159, <http://dx.doi.org/10.36418/Jist.V3i11.5>

- Muhammad Nuh Al-Azhar, *Digital Forensic Panduan Praktis Investigasi Komputer*, (Jakarta: Salemba Infotek, 2021),
- Nelson, B., Phillips, A., & Steuart, C. “*Guide to Computer Forensics and Investigations*”, 2020, Cengage Learning. Topo Santoso, *Hukum Pidana: Suatu Pengantar*, 1 (Depok: Rajawali Pers, 2021). (Depok: Rajawali Pers, 2021).
- Nita Azhar “Tahapan Dan Teknik Forensik Digital Dalam Mengungkap Kejahatan Dunia Maya” IDS Digital College <https://ids.ac.id/Tahapan-Dan-Teknik-Forensik-Digital-Dalam-Dunia-Maya/>
- Pasal 13 Ayat (2) Peraturan Menteri Komunikasi Dan Informatika Nomor 10 Tahun 2021 Tentang Perubahan Atas Peraturan Menteri Komunikasi Dan Informatika Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privasi
- Pasal 14 Ayat (1) Peraturan Menteri Komunikasi Dan Informatika Nomor 10 Tahun 2021 Tentang Perubahan Atas Peraturan Menteri Komunikasi Dan Informatika Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privasi
- Pasal 14 Ayat (2) Peraturan Menteri Komunikasi Dan Informatika Nomor 10 Tahun 2021 Tentang Perubahan Atas Peraturan Menteri Komunikasi Dan Informatika Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat
- Pasal 37 Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual
- Pasal 68 Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual
- Pasal 69 Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual
- Pasal 7 Ayat (2) Undang-Undang Nomor 31 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi Dan Korban
- Pasal 70 Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual
- Tzu-Wei Hung And Chun-Ping Yen, “On The Person-Based Predictive Policing Of AI,” *Ethics And Information Technology* 23 (2025): 165–76, <https://doi.org/10.1007/S10676-020-09539-X>.
- Widodo, Prabowo P. Dkk, “*Pemodelan System Berorientasi Obyek Dengan UML*”, (Yogyakarta: Graha Ilmu, 2011). Homas C. King, “*Artificial Intelligence Crime: An Interdisciplinary Analysis Of Foreseeable Threats And Solutions*”, *Sci Eng Ethics* 26, <https://doi.org/10.1007/S11948-018-00081-0> Diakses 21 Desember 2024.
- Yusuf, "Perlu Pemahaman Bersama Terkait Pengembangan AI Di Indonesia," Ditjen Aptika Kominfo, 21 Februari 2020, <https://aptika.kominfo.go.id/2020/02/Perlu-Pemahaman-Bersama-Tentang-Pengembangan-Ai-Di-Indonesia/> Diakses Desember 2024
- Mansur, Arief & Gultom, “Cyber Law Aspek Hukum Teknologi Informasi”, PT Refika Aditama, Bandung :2005.
- Zaky Al-Yamani Fakta Mengejutkan Di Balik Kasus Video Porno Berteknologi *Deepfake* Yang Diungkap Polres Kendal <https://www.viva.co.id/Trending/1829272-5-Fakta-Mengejutkan-Di-Balik-Kasus-Video-Porno-Berteknologi-Deepfake-Yang-Diungkap-Polres-Kendal>.