Jurnal Serambi Hukum
Vol 18 No 01 Tahun 2025
e-ISSN: 2549-5275
p-ISSN: 1693-0819

Penegakan Hukum Terhadap Penyalahgunaan *Deepfake* Pada Pornografi Anak Di Era *Artifical Intelegence* di Indonesia

Muh. Taufik Darmawan, Amir Junaidi, Ariy Khaerudin
Fakultas Hukum Magister Hukum Universitas Islam Batik Surakarta
Email: muhtaufikdarmawan@gmail.com

ABSTRACT

The development of Artificial Intelligence (AI) technology has had a significant impact on various aspects of life, including the emergence of deepfake technology. This technology enables realistic manipulation of digital content, including for the creation of illegal content such as child pornography. This phenomenon poses serious challenges in law enforcement, especially in Indonesia which is facing an increase in cases of digital child exploitation. This research aims to examine the legal aspects related to deepfake child pornography in Indonesia, identify challenges to law enforcement, and provide recommendations to strengthen legal regulations and implementation. The method used is normative juridical research with a legislative and comparative approach. The data analysed includes regulations such as Law No. 44/2008 on Pornography and Law No. 11/2008 on Electronic Information and Transactions (ITE). The results show that although Indonesia has regulations governing pornography and electronic transactions, there are no specific rules that explicitly cover deepfake child pornography. The main challenges include technological limitations on the part of law enforcement, difficulty in identifying perpetrators, and collecting and proving digital evidence in court. Recommendations include updating regulations to cover AI-based crimes, increasing the capacity of law enforcement through technology training, and digital literacy campaigns for the public. In addition, international cooperation is also needed to face this global challenge. This research is expected to contribute to policy development and law enforcement efforts against deepfake child pornography in Indonesia.

Keywords: Deepfake, Child Pornography, Artificial Intelligence

ABSTRAK

Perkembangan teknologi Artificial Intelligence (AI) telah membawa dampak signifikan pada berbagai aspek kehidupan, termasuk kemunculan teknologi deepfake. Teknologi ini memungkinkan manipulasi konten digital secara realistis, termasuk untuk pembuatan konten ilegal seperti pornografi anak. Fenomena ini memunculkan tantangan serius dalam penegakan hukum, terutama di Indonesia yang menghadapi peningkatan kasus eksploitasi anak secara digital. Penelitian ini bertujuan untuk mengkaji aspek hukum terkait deepfake pornografi anak di Indonesia, mengidentifikasi tantangan penegakan hukum, serta memberikan rekomendasi untuk memperkuat regulasi dan implementasi hukum. Metode yang digunakan adalah penelitian yuridis normatif dengan pendekatan perundang-undangan dan komparatif. Data yang dianalisis meliputi regulasi seperti Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Hasil penelitian menunjukkan bahwa meskipun Indonesia memiliki regulasi yang mengatur pornografi dan transaksi elektronik, belum ada aturan khusus yang secara eksplisit mencakup deepfake pornografi anak. Tantangan utama meliputi keterbatasan teknologi di pihak penegak hukum, kesulitan identifikasi pelaku, serta pengumpulan dan pembuktian bukti digital di pengadilan. Sebagai rekomendasi, diperlukan pembaruan regulasi yang mencakup kejahatan berbasis AI, peningkatan kapasitas penegak hukum melalui

pelatihan teknologi, dan kampanye literasi digital untuk masyarakat. Selain itu, kerja sama internasional juga diperlukan untuk menghadapi tantangan global ini. Penelitian ini diharapkan dapat memberikan kontribusi pada pengembangan kebijakan dan upaya penegakan hukum terhadap deepfake pornografi anak di Indonesia.
Kata Kunci: Deepfake, Pornografi Anak, Artificial Intelligence

A. PENDAHULUAN

Perkembangan teknologi Artificial Intelligence (AI) secara signifikan telah mengubah lanskap keamanan siber dan dunia hukum di seluruh dunia. Kemampuan AI dalam mengolah data dalam skala besar dan menjalankan tugas kompleks dengan efisiensi tinggi memberikan manfaat besar bagi banyak sektor, seperti bisnis, pendidikan, dan pelayanan publik. Namun, di sisi lain, kemajuan ini juga membuka peluang bagi tindakan kriminal yang memanfaatkan teknologi AI untuk merancang, menyebarkan, atau mengeksekusi kejahatan dunia maya (*cybercrime*) yang lebih canggih dan sulit ditelusuri. Penerapan AI dalam cybercrime termasuk dalam kategori kejahatan berbasis komputer (*computer-related crime*). Melalui pemrograman khusus, AI dapat digunakan untuk menciptakan malware, perangkat lunak peretas, atau serangan otomatis yang menargetkan individu maupun institusi. Bahkan, kejahatan AI tidak hanya bersifat domestik, melainkan lintas batas negara sehingga menyulitkan otoritas lokal dalam penegakan hukum. Seiring dengan tingginya tingkat ketergantungan masyarakat terhadap internet, risiko kejahatan berbasis AI ini pun meningkat pesat, mengakibatkan kebutuhan mendesak akan regulasi dan pengaturan hukum yang komprehensif dalam rangka melindungi data dan keamanan publik dari potensi penyalahgunaan teknologi ini.[1]

Dalam era revolusi industri 4.0, teknologi telah mengalami perkembangan yang luar biasa cepat dan signifikan, salah satunya adalah kemajuan dalam bidang Artificial Intelligence (AI) atau kecerdasan buatan. AI telah menjadi bagian integral dalam kehidupan manusia, memberikan berbagai manfaat yang mencakup efisiensi kerja, otomatisasi proses, hingga kemampuan untuk menganalisis data dalam jumlah besar. Namun, di balik semua keuntungannya, AI juga membawa tantangan baru, khususnya dalam konteks keamanan siber atau cybercrime. Di Indonesia, regulasi terkait kejahatan siber sudah ada dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), namun penerapannya masih terfokus pada kejahatan dunia maya secara umum, belum secara spesifik mengatur penggunaan AI dalam kejahatan ini. Studi menunjukkan bahwa penggunaan AI dalam tindak pidana penyebaran malware, misalnya, sulit dikendalikan karena sifat teknologi AI yang mampu beradaptasi dan berkembang, sehingga pelaku kejahatan dapat terus memperbarui teknik dan strategi mereka untuk menghindari deteksi. Penggunaan AI dalam cybercrime membutuhkan analisis yuridis lebih mendalam untuk memastikan efektivitas hukum dan perlindungan yang memadai.[2]

Teknologi deepfake adalah salah satu inovasi yang muncul dari kemajuan pesat dalam bidang kecerdasan buatan (AI) dan pembelajaran mendalam. Deepfake memungkinkan

[1] Afrizal Mukti Wibowo Timothy Adrianus P Gultom, Diah Pawestri Maharani, "Analisis Yuridis Penggunaan Artificial Intelligence Yang Menjalankan Fungsi Legal Audit Dalam Regulatory Compliance System Di Indonesia: The Juridical Analysis of the Use of Artificial Intelligence Performing Legal Audit Function in Regulatory Compliance," *Brawijaya Law Student Journal*, March 18, 2024, https://hukum.studentjournal.ub.ac.id/index.php/hukum/article/view/5809.

[2] Fatmawati and Raihana Raihana, "Analisis Yuridis Terhadap Artificial Intelligence Pada Tindak Pidana Penyebaran Malware Di Indonesia," *INNOVATIVE Journal Of Social Science Research* 3 (June 18, 2023): 12190–201.

manipulasi konten visual dan audio untuk menciptakan media yang sangat realistis namun palsu, seperti video atau gambar yang menampilkan seseorang melakukan atau mengatakan sesuatu yang sebenarnya tidak pernah terjadi.[3] Teknologi ini memanfaatkan algoritma AI untuk menggantikan wajah atau suara seseorang dengan orang lain, menghasilkan konten yang sulit dibedakan dari yang asli oleh pengamat manusia.[4] Meskipun awalnya digunakan dalam konteks hiburan dan seni, deepfake kini menjadi perhatian serius karena potensi penyalahgunaannya dalam menyebarkan informasi palsu dan propaganda.[5]

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.[6] Selain itu, deepfake juga telah menemukan aplikasi dalam bidang pemasaran, komunikasi politik, dan media, di mana ia dapat digunakan untuk membuat konten yang lebih menarik dan personal.[7] Namun, kemudahan pembuatan deepfake juga menimbulkan ancaman terhadap privasi dan keamanan, karena dapat digunakan untuk menciptakan berita palsu atau merusak reputasi individu.[8]

Di satu sisi, AI membantu aparat penegak hukum dalam mengidentifikasi pola kejahatan, memprediksi tindakan kriminal, dan meningkatkan efisiensi penyelidikan. Namun, di sisi lain, AI juga digunakan oleh pelaku kejahatan untuk melakukan serangan siber yang lebih canggih, seperti serangan phishing berbasis AI, deepfake, dan ransomware yang menggunakan algoritma pembelajaran mesin untuk menghindari deteksi. Penggunaan AI dalam cybercrime menimbulkan sejumlah tantangan hukum yang kompleks. Pertama, penggunaan AI oleh pelaku kejahatan sering kali melibatkan teknik yang sangat canggih dan sulit dideteksi, sehingga mempersulit aparat penegak hukum dalam mengidentifikasi dan menangkap pelaku. Kedua, AI dapat digunakan untuk mengaburkan jejak digital, membuat pelacakan menjadi lebih sulit dan menambah kesulitan dalam proses pembuktian hukum. Ketiga, regulasi yang ada saat ini sering kali belum memadai untuk menangani kejahatan yang melibatkan AI, karena undang-undang yang ada belum disesuaikan dengan perkembangan teknologi terbaru.

Hal ini menimbulkan kekosongan hukum yang dapat dimanfaatkan oleh pelaku kejahatan siber. Selain itu, masalah etika juga menjadi perhatian utama dalam penggunaan AI, baik oleh pihak berwenang maupun oleh pelaku kejahatan. AI memiliki kemampuan untuk belajar dan beradaptasi dengan cepat, tetapi tidak memiliki kapasitas moral atau etika. Dalam tangan yang salah, AI dapat digunakan untuk tujuan yang merugikan, seperti menciptakan konten palsu (deepfake) yang dapat merusak reputasi seseorang atau bahkan menimbulkan kekacauan sosial. Pada saat yang sama, penggunaan AI oleh aparat penegak

[3] H Shahzad et al., "A Review of Image Processing Techniques for Deepfakes," *Sensors (Basel, Switzerland)* 22 (2022), https://doi.org/10.3390/s22124556.
[4] Saiyad Mahmmadakram Hanif and Vivek Dave, "Deepfakes Technology Using AI," *International Journal of Scientific Research in Science, Engineering and Technology*, 2022, https://doi.org/10.32628/ijsrset229522.
[5] M Rana et al., "Deepfake Detection: A Systematic Literature Review," *IEEE Access* 10 (2022): 25494–513, https://doi.org/10.1109/access.2022.3154404.
[6] 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.
[7] Büşra Kiliç and Mehmet Emin Kahraman, "Current Usage Areas of Deepfake Applications with Artificial Intelligence Technology," *İletişim ve Toplum Araştırmaları Dergisi*, 2023, https://doi.org/10.59534/jcss.1358318.
[8] Jayanta Kumar Panda and Rajnandini Panigrahy, "Unmasking Deception In The Age Of Artificial Intelligence: A Comprehensive Analysis Of Indian Celebrity's Deepfakes News," *ShodhKosh: Journal of Visual and Performing Arts*, 2023, https://doi.org/10.29121/shodhkosh.v4.i2.2023.2268.

hukum juga harus dilakukan dengan hati-hati untuk menghindari pelanggaran terhadap hak asasi manusia, seperti hak privasi dan kebebasan berekspresi.[9]

Analisis yuridis mengenai penggunaan AI dalam cybercrime juga harus mempertimbangkan peran dan tanggung jawab dari berbagai pihak yang terlibat. Dalam hal ini, bukan hanya pelaku kejahatan yang harus bertanggung jawab, tetapi juga para pengembang teknologi dan penyedia layanan digital yang memungkinkan terjadinya kejahatan tersebut. Pertanyaan-pertanyaan mengenai siapa yang harus bertanggung jawab jika AI melakukan kesalahan atau jika AI digunakan untuk melakukan kejahatan juga menjadi isu yang krusial dan memerlukan pembahasan mendalam. Selain itu, peran pemerintah dan lembaga internasional dalam mengatur dan mengawasi penggunaan AI juga sangat penting. Di era globalisasi, cybercrime sering kali melibatkan berbagai yurisdiksi, sehingga diperlukan kerjasama internasional yang kuat untuk menanggulangi kejahatan ini.

Pemerintah perlu merumuskan kebijakan yang tepat untuk mengatur penggunaan AI, baik dalam konteks penegakan hukum maupun dalam pencegahan kejahatan siber. Pada saat yang sama, kerjasama internasional juga harus diperkuat untuk memastikan bahwa hukum dapat diterapkan secara efektif di seluruh dunia. Dalam konteks Indonesia, penerapan AI dalam penegakan hukum masih dalam tahap awal. Meskipun pemerintah telah mengakui pentingnya AI dalam menghadapi tantangan kejahatan siber, implementasi teknologinya masih terbatas dan regulasinya belum sepenuhnya siap untuk menghadapi berbagai tantangan yang ada. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang menjadi dasar hukum penanganan cybercrime di Indonesia perlu ditinjau dan disesuaikan dengan perkembangan teknologi, termasuk AI. Pendekatan yuridis dalam menangani penggunaan AI dalam cybercrime juga harus melibatkan berbagai disiplin ilmu, seperti ilmu komputer, etika, dan kriminologi.

Seiring dengan meningkatnya penggunaan deepfake, upaya untuk mendeteksi dan mengatasi dampaknya juga semakin berkembang. Berbagai metode deteksi deepfake telah dikembangkan, termasuk teknik pembelajaran mendalam dan pembelajaran mesin yang dirancang untuk mengidentifikasi manipulasi wajah dalam video dan gambar.[10] Selain itu, peningkatan literasi digital dan kesadaran publik tentang bahaya deepfake menjadi penting untuk melawan disinformasi yang disebabkan oleh konten sintetis ini. Dengan kolaborasi antara teknologi, regulasi, dan pendidikan, diharapkan ancaman yang ditimbulkan oleh deepfake dapat diminimalisir, menjaga integritas informasi di era digital.

Analisis yuridis mengenai penggunaan AI dalam cybercrime harus mampu mengidentifikasi potensi risiko, memberikan solusi yang tepat, dan memastikan bahwa hukum dapat berfungsi secara efektif dalam menghadapi tantangan yang ada. Untuk mencapai hal tersebut, diperlukan upaya yang berkesinambungan dari berbagai pihak, termasuk pemerintah, aparat penegak hukum, pengembang teknologi, dan masyarakat. Hanya dengan kerjasama yang baik dan regulasi yang tepat, kita dapat memastikan bahwa perkembangan teknologi, termasuk AI, dapat digunakan untuk kebaikan dan tidak disalahgunakan untuk tujuan yang merugikan. Sebagai negara yang sedang berkembang, Indonesia perlu terus memperkuat regulasi dan infrastruktur hukumnya agar dapat mengikuti perkembangan teknologi dan menghadapi tantangan cybercrime di masa depan.

[9] D T Rachmadie, "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016," *Jurnal Hukum Pidana Dan Penanggulangan Kejahatan* 9, no. 2 (2016): 128–36, https://jurnal.uns.ac.id/recidive/article/view/47400.

[10] Supriya et al., "Investigating the Evolving Landscape of Deepfake Technology: Generative AI's Role in It's Generation and Detection," *International Research Journal on Advanced Engineering Hub (IRJAEH)*, 2024, https://doi.org/10.47392/irjaeh.2024.0206.

Analisis yuridis mengenai penggunaan AI dalam cybercrime juga harus diimbangi dengan edukasi kepada masyarakat mengenai risiko dan bahaya dari penggunaan AI yang tidak bertanggung jawab. Edukasi ini penting untuk meningkatkan kesadaran masyarakat dan membangun budaya yang lebih aman dalam penggunaan teknologi. Dengan demikian, kita dapat menciptakan lingkungan digital yang lebih aman dan terlindungi dari ancaman kejahatan siber yang semakin kompleks. Dalam penutup, penting untuk diingat bahwa teknologi, termasuk AI, adalah alat yang netral. Penggunaannya tergantung pada tangan siapa teknologi tersebut berada. Oleh karena itu, regulasi yang tepat dan etika yang kuat harus menjadi landasan dalam penggunaan AI, khususnya dalam konteks cybercrime. Dengan pendekatan yuridis yang komprehensif dan kolaborasi yang baik antar berbagai pihak, kita dapat memanfaatkan teknologi AI untuk kepentingan yang positif dan mencegahnya dari disalahgunakan untuk kejahatan siber.

Melihat kebutuhan regulasi dan pemahaman hukum yang mendalam dalam menghadapi kejahatan berbasis AI, latar belakang penelitian ini penting untuk memberikan kajian mendalam atas penggunaan AI dalam cybercrime. Analisis ini akan mencakup sejauh mana regulasi yang ada dapat menjawab tantangan teknologi AI, perlindungan terhadap korban, serta dampak hukum bagi pelaku kejahatan yang menggunakan AI. Pemahaman ini diharapkan dapat mendorong pembuat kebijakan untuk mengembangkan regulasi yang tidak hanya mencakup tindakan preventif, tetapi juga menciptakan kerangka hukum yang adaptif dan dapat merespon perubahan cepat dalam teknologi informasi dan keamanan dunia maya.[11]

B. METODE PENELITIAN

Penelitian (*research*) merupakan rangkaian kegiatan ilmiah dalam rangka pemecahan suatu permasalahan. Hasil penelitian tidak pernah dimaksudkan sebagai suatu pemecahan (solusi) langsung bagi permasalahan yang dihadapi. Karena penelitian merupakan bagian saja dari usaha pemecahan masalah yang lebih besar. Fungsi penelitian adalah mencarikan penjelasan dan jawaban terhadap permasalahan serta memberikan alternatif bagi kemngkinan yang dapat digunakan untuk pemecahan masalah.[12] Penelitian ini menggunakan pendekatan yuridis normatif, dengan metode analisis hukum yang menekankan pada studi pustaka untuk mengidentifikasi peraturan perundang-undangan, yurisprudensi, dan konsep hukum yang berkaitan dengan penggunaan Artificial Intelligence (AI) dalam tindakan Deepfake Pornografi. Pendekatan ini bertujuan untuk memahami dan menganalisis aspek hukum yang berkaitan dengan pemanfaatan teknologi AI, baik sebagai alat maupun subjek dalam tindak pidana Deepfake Pornografi. Teknik pengumpulan data yang digunakan peneliti adalah metode *library research*, yaitu studi kepustakaan.

Metode analisis kualitatif dengan pendekatan deskriptif-analitis, di mana data yang diperoleh diinterpretasikan untuk menggambarkan kondisi hukum yang ada dan menentukan arah kebijakan hukum terkait pemanfaatan AI dalam cybercrime. Analisis ini mencakup: Pendekatan Perundang-undangan (*Statute Approach*): Meninjau peraturan hukum nasional dan internasional terkait *Deepfake* Pornografi dan penggunaan AI dalam hukum pidana; Pendekatan Konseptual (*Conceptual Approach*): Menelaah konsep-konsep utama tentang *Deepfake* Pornografi dan teknologi AI dalam hukum; Pendekatan Kasus

[11] Fatmawati and Raihana, "Analisis Yuridis Terhadap Artificial Intelligence Pada Tindak Pidana Penyebaran Malware Di Indonesia."
[12] Saifuddin Anwar, *Metode Penelitian*, Cet. III (Yogyakarta: Pustaka Pelajar Offset, 2016).

(*Case Approach*): Mengkaji putusan pengadilan yang relevan untuk melihat bagaimana AI diposisikan dalam kasus *Deepfake* Pornografi.

C. HASIL DAN PEMBAHASAN

1. Analisis Legalitas *Deepfake* Pornografi Anak di Indonesia

Deepfake pornografi anak merujuk pada konten yang dihasilkan secara algoritmik di mana wajah seorang anak disuperimposisikan ke tubuh orang lain dalam konteks pornografi. Teknologi ini memanfaatkan model pembelajaran mendalam seperti *generative adversarial networks* (GANs) dan *autoencoders* untuk menciptakan gambar atau video yang sangat realistis.[13] Konten semacam ini sering kali dibuat tanpa persetujuan dari individu yang wajahnya digunakan, menjadikannya bentuk eksploitasi dan pelecehan yang serius.[14] Hal ini menimbulkan kekhawatiran besar karena dapat digunakan untuk membuat konten pornografi anak yang sangat merugikan.

Teknologi *deepfake* menggunakan teknik manipulasi wajah seperti pertukaran wajah dan rekombinasi ekspresi wajah. Teknik ini telah berkembang menjadi sangat canggih, memungkinkan pembuatan gambar dan video yang hampir tidak dapat dibedakan dari yang asli. Dengan memanfaatkan koleksi gambar yang besar, teknologi ini dapat menciptakan representasi visual yang sangat realistis dari individu yang ditargetkan. Untuk mengatasi ancaman yang ditimbulkan oleh *deepfake* pornografi anak, diperlukan pengembangan kerangka kerja yang kuat untuk mengidentifikasi gambar dan video *deepfake*. Algoritma pembelajaran mesin dapat digunakan untuk mendeteksi deepfake dengan menganalisis dataset visual yang ada dan melakukan analisis komparatif terhadap teknik deteksi yang berbeda. Upaya ini penting untuk membedakan antara konten asli dan yang dimanipulasi, serta untuk mencegah penyebaran lebih lanjut dari konten yang merugikan ini.

Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi di Indonesia telah menjadi subjek analisis dan diskusi yang mendalam. UU ini muncul sebagai respons terhadap kekhawatiran masyarakat mengenai penyebaran konten pornografi yang semakin meluas dan mudah diakses melalui media elektronik dan komunikasi.[15] Salah satu isu utama yang diangkat adalah bagaimana tindakan mengakses konten pornografi dapat dikategorikan sebagai pelanggaran hukum, yang menunjukkan perlunya perubahan dalam undang-undang untuk memasukkan tindakan akses tersebut.[16] Selain itu, UU ini juga menghadapi tantangan dalam penerapannya, terutama dalam hal definisi dan interpretasi yang dapat bervariasi berdasarkan keragaman budaya di Indonesia.[17]

---

[13] Manoj Kumar, Praveen Kumar Rai, and Pankaj Kumar, "A Novel Approach for Detecting Deepfake Face Using Machine Learning Algorithms," *2024 2nd International Conference on Disruptive Technologies (ICDT)*, 2024, 1588–92, https://doi.org/10.1109/ICDT61202.2024.10489036.

[14] Vasileia Karasavva and Aalia Noorbhai, "The Real Threat of Deepfake Pornography: A Review of Canadian Policy," *Cyberpsychology, Behavior and Social Networking* 24 3 (2021): 203–9, https://doi.org/10.1089/cyber.2020.0272.

[15] Muhammad Iqbal Wibisono and Bahrul Fawaid, "Larangan Pornografi Dalam Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi (Perspektif Asas Legalitas)," *QISTIE*, 2022, https://doi.org/10.31942/jqi.v14i2.6084.

[16] Nynda Fatmawati Octarina and M Hasan, "The Urgency of Regulating Access to Pornography Content in Law No. 44 of 2008 Concerning Pornography," *International Journal of Science and Society*, 2023, https://doi.org/10.54783/ijsoc.v5i1.643.

[17] M Murdan, "Membaca Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi Dari Perspektif Sosiologi Hukum," *Indonesian Journal of Shariah and Justice*, 2021, https://doi.org/10.46339/ijsj.v1i1.5.

Selain itu, UU Pornografi ini juga dikritik karena kurangnya kejelasan dalam formulasi sanksi pidana, yang dapat menyebabkan ketidakpastian hukum.[18] Implementasi penegakan hukum juga menghadapi berbagai hambatan, termasuk faktor undang-undang itu sendiri, penegak hukum, dan masyarakat.[19] Meskipun demikian, UU ini bertujuan untuk melindungi generasi muda dari dampak negatif pornografi dan menjaga nilai-nilai etika dan kemanusiaan dalam masyarakat.[20] Namun, untuk mencapai tujuan tersebut, diperlukan perbaikan dalam undang-undang agar tidak menimbulkan interpretasi ganda dalam tahap pelaksanaannya.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) merupakan landasan hukum penting dalam mengatur aktivitas di dunia maya di Indonesia. Namun, sejak diberlakukan, UU ITE ini menghadapi berbagai kritik terkait dengan ketidakpastian hukum dan potensi penafsiran ganda yang dapat mengarah pada kriminalisasi yang tidak tepat. Beberapa pasal, seperti Pasal 27, 28, dan 29, sering kali menjadi sumber kontroversi karena dianggap memiliki interpretasi yang beragam, yang dapat menimbulkan perbedaan persepsi di kalangan penegak hukum. Untuk mengatasi masalah ini, pemerintah melakukan revisi pertama melalui UU No. 19 Tahun 2016, namun perubahan tersebut belum sepenuhnya menjawab permasalahan yang ada, sehingga dilakukan revisi kedua dengan UU No. 1 Tahun 2024.[21]

Relevansi hukum pidana dalam mengatur kejahatan deepfake pornografi anak sangat penting mengingat dampak serius yang ditimbulkan oleh teknologi ini. Deepfake, yang memungkinkan manipulasi gambar dan video untuk menciptakan konten pornografi yang tampak nyata, menimbulkan ancaman signifikan terhadap privasi dan keamanan individu, terutama anak-anak. Teknologi ini dapat digunakan untuk membuat konten pornografi anak yang tidak hanya melanggar hak asasi manusia tetapi juga merusak moral sosial dan kepentingan publik.[22] Selain itu, penegakan hukum pidana terhadap deepfake pornografi anak juga memerlukan pendekatan yang komprehensif dan kolaboratif. Hal ini mencakup pengembangan kriteria yang jelas untuk mengidentifikasi deepfake yang berbahaya, serta solusi teknologi untuk mendeteksi dan menghapus konten tersebut secara cepat.[23] Kerjasama antara sektor publik dan swasta, serta pelatihan bagi penegak hukum dan pemangku kepentingan lainnya, juga sangat penting untuk meningkatkan efektivitas penegakan hukum.[24]

---

[18] Z Rahmat, "Localism Principle in the Formulation of Indonesian Regulations on Pornography" 12 (2020): 167–77, https://doi.org/10.18196/jkm.122045.

[19] Dicky Putra Arumawan and S Iksan, "Implementasi Penegakan Sanksi Pidana Dalam Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi (Studi Kasus Di Wilayah Hukum Pengadilan Negeri Boyolali)," 2016, https://consensus.app/papers/implementasi-penegakan-sanksi-pidana-dalam-undangundang-arumawan-iksan/36967d0de13554548bba83cef208b23c/.

[20] Ratu Agung Dewangga Arinatha Gunawan, Nyoman Gede Sugiartha, and Ni Made Sukaryati Karma, "Penyebaran Iklan Pada Media Elektronik Yang Memuat Konten Pornografi," *Jurnal Interpretasi Hukum*, 2021, https://doi.org/10.22225/juinhum.2.2.3421.261-267.

[21] Agus Purwono et al., "IMPLICATIONS AND CONSIDERATIONS OF THE NEW ELECTRONIC INFORMATION AND TRANSACTION LAW," *ANAYASA : Journal of Legal Studies*, 2024, https://doi.org/10.61397/ays.v1i2.242.

[22] Nataša Mrvić-Petrović, "Criminal Law Approach to Regulating Non-Consensual Pornographic Deepfake," *Bezbednost, Beograd*, 2024, https://doi.org/10.5937/bezbednost2402005p.

[23] Marina Efremova and E Russkevich, "Deepfake And Criminal Law," *Bulletin of the Kazan Law Institute of MIA Russia*, 2024, https://doi.org/10.37973/vestnikkui-2024-56-13.

[24] Dwi Nurfauziah Ahmad and Latifatul Hidayati, "LAW ENFORCEMENT AGAINST CRIMINAL ACTORS OF CHILD PORNOGRAPHY THROUGH SOCIAL MEDIA," *JHR (Jurnal Hukum Replik)*, 2021, https://doi.org/10.31000/JHR.V9I1.4120.

Dengan demikian, hukum pidana tidak hanya berfungsi sebagai alat pencegahan tetapi juga sebagai sarana untuk memberikan keadilan bagi korban dan melindungi masyarakat dari ancaman yang ditimbulkan oleh deepfake pornografi anak.

Perlindungan hukum terhadap korban, khususnya anak-anak, dalam konteks *deepfake*, menjadi semakin penting seiring dengan perkembangan teknologi yang memungkinkan manipulasi gambar dan video secara realistis. *Deepfake*, yang sering digunakan untuk tujuan pornografi tanpa persetujuan orang yang bersangkutan, menimbulkan ancaman serius terhadap privasi dan reputasi individu, termasuk anak-anak.[25] Di Indonesia, hukum perlindungan anak mencakup berbagai aspek mulai dari hak sipil hingga eksploitasi ekonomi dan sosial. Namun, cakupan hukum yang luas ini sering kali menimbulkan kekosongan hukum yang memerlukan reformasi agar perlindungan anak menjadi prioritas negara.[26]

Untuk mengatasi celah hukum ini, beberapa penelitian menyarankan penggunaan konsep "Hak Untuk Dilupakan" (*Right to be Forgotten*) sebagai upaya perlindungan hukum bagi korban deepfake pornografi di Indonesia.[27] Namun, implementasi konsep ini masih menghadapi tantangan, seperti kurangnya prosedur yang jelas dalam UU ITE dan ketidakefektifan otoritas dalam menangani kasus *deepfake* pornografi. Oleh karena itu, diperlukan studi komparatif dengan negara lain yang telah menerapkan RTBF untuk kejahatan siber, termasuk *deepfake* pornografi, guna memperbaiki regulasi dan memberikan perlindungan yang lebih baik bagi korban.

2. Tantangan Penegakan Hukum terhadap Deepfake Pornografi Anak

Deteksi dan pembuktian keaslian konten *deepfake* menghadapi berbagai tantangan teknis yang signifikan. Salah satu tantangan utama adalah kemampuan generalisasi dari model deteksi *deepfake*. Banyak model deteksi yang ada saat ini dilatih untuk mengenali jenis deepfake tertentu, sehingga kesulitan dalam mendeteksi *deepfake* yang dihasilkan dengan teknik yang berbeda. Selain itu, deteksi *deepfake* di dunia nyata sering kali menghadapi kesulitan seperti pengelolaan video dengan banyak orang dalam satu adegan atau pengenalan gerakan wajah yang bergerak mendekati atau menjauhi kamera.[28] Tantangan lain dalam mendeteksi *deepfake* adalah tingkat realisme yang tinggi dari konten yang dihasilkan. Teknologi *deep learning* yang digunakan untuk membuat *deepfake* telah mencapai tingkat realisme yang sangat tinggi, sehingga sulit bagi manusia untuk membedakan antara konten palsu dan asli hanya dengan mata telanjang. Hal ini diperparah dengan ketersediaan perangkat lunak yang dapat diakses secara bebas di internet, memungkinkan individu tanpa keahlian khusus untuk

---

[25] Valéria Sousa-Gomes et al., "Psychological Intervention and Treatment Programs for Adult Victims of Child Sexual Abuse: A Systematic Review.," *Psychological Trauma : Theory, Research, Practice and Policy*, 2022, https://doi.org/10.1037/tra0001389.

[26] Sri Yunarti et al., "Internasional Conference on Humanity, Law and Sharia (ICHLaSh). November 14-15. 2018 Reconstruction on Sharia Sciences in Facing Contemporary Law Problematics/97 EXAMINATION OF CONSTITUTIONALITY OF CHILD PROTECTION LAW IN FIQH," 2020, https://consensus.app/papers/internasional-conference-on-humanity-law-and-sharia-yunarti-syakir/7134f16f511955a9abc90f866defeb7a/.

[27] Muhammad Deckri Algamar and Aliya Ilysia Irfana Ampri, "Hak Untuk Dilupakan: Penghapusan Jejak Digital Sebagai Perlindungan Selebriti Anak Dari Bahaya Deepfake," *JURNAL YUSTIKA: MEDIA HUKUM DAN KEADILAN*, 2022, https://doi.org/10.24123/yustika.v25i01.5091.

[28] D Coccomini, "Deepfake Detection: Challenges and Solutions," 2023, 688–89, https://consensus.app/papers/deepfake-detection-challenges-and-solutions-coccomini/e1b9d4babc1f50799ba4247904e10509/.

membuat gambar dan video palsu yang sangat realistis. Oleh karena itu, diperlukan alat otomatis yang mampu mendeteksi konten multimedia palsu dan mencegah penyebaran informasi palsu yang berbahaya.[29]

Selain itu, AI juga digunakan dalam strategi "*predictive policing*" yang bertujuan untuk memprediksi lokasi dan waktu kejahatan berikutnya berdasarkan analisis data.[30] Namun, adopsi strategi ini sering kali melampaui temuan ilmiah yang sudah mapan, menimbulkan perdebatan tentang efektivitas dan dampak potensial dari teknik-teknik baru ini.

Praktik anonimitas di internet sering kali dimanfaatkan oleh pelaku kejahatan siber seperti pencucian uang, perdagangan narkoba, terorisme, dan pornografi anak. Dengan menggunakan alat dan pengetahuan yang tersedia di internet, para pelaku dapat berkomunikasi dan bertukar informasi dengan risiko yang lebih rendah terhadap identifikasi pribadi mereka. Hal ini menimbulkan tantangan bagi penegak hukum untuk menemukan keseimbangan antara kebebasan berbicara, privasi, dan kebutuhan untuk mengidentifikasi pelaku kejahatan.[31] Di media sosial, anonimitas memungkinkan pengguna untuk membuat profil palsu yang dapat digunakan untuk menyebarkan informasi yang menyesatkan atau menyerang individu lain. Misalnya, di platform seperti Twitter, pengguna dapat membuat akun anonim untuk melakukan perundungan siber atau menyebarkan berita palsu. Metodologi deteksi profil palsu telah dikembangkan untuk mengatasi masalah ini, namun tantangan tetap ada dalam mengaitkan profil anonim dengan identitas nyata.[32]

Penggunaan teknologi untuk menyembunyikan jejak pelaku kejahatan telah menjadi perhatian utama dalam penegakan hukum. Pelaku kejahatan memanfaatkan berbagai teknologi untuk menyembunyikan komunikasi dan bukti yang tersimpan di komputer dari pihak berwenang. Teknologi seperti enkripsi, kata sandi, kompresi digital, steganografi, penyimpanan jarak jauh, dan penonaktifan audit sering digunakan untuk tujuan ini. Selain itu, alat dan teknik anonimitas seperti remailer anonim, uang digital anonim, dan telepon seluler kloning juga digunakan untuk menyembunyikan jejak kejahatan. Penggunaan teknologi ini oleh pelaku kejahatan dan teroris telah mempengaruhi investigasi dan penuntutan, dan penegak hukum harus mengembangkan strategi untuk mengatasi tantangan ini, terutama dalam hal enkripsi.[33] Secara keseluruhan, penggunaan teknologi untuk menyembunyikan jejak pelaku kejahatan menimbulkan tantangan signifikan bagi penegakan hukum dan memerlukan pendekatan yang inovatif untuk mengatasi hambatan ini.

Masalah bukti digital dalam kasus *deepfake* menjadi tantangan signifikan dalam era kejahatan siber. *Deepfake*, yang merupakan hasil dari algoritma kecerdasan buatan, telah diidentifikasi sebagai ancaman serius terhadap keamanan siber karena kemampuannya untuk menciptakan media palsu yang sangat realistis. Tantangan utama

[29] L Verdoliva, "Media Forensics and DeepFakes: An Overview," *IEEE Journal of Selected Topics in Signal Processing* 14 (2020): 910–32, https://doi.org/10.1109/JSTSP.2020.3002101.
[30] Tzu-Wei Hung and Chun-Ping Yen, "On the Person-Based Predictive Policing of AI," *Ethics and Information Technology* 23 (2020): 165–76, https://doi.org/10.1007/s10676-020-09539-x.
[31] H Armstrong and Patrick Forde, "Internet Anonymity Practices in Computer Crime," *Inf. Manag. Comput. Secur.* 11 (2003): 209–15, https://doi.org/10.1108/09685220310500117.
[32] Patxi Galán-García et al., "Supervised Machine Learning for the Detection of Troll Profiles in Twitter Social Network: Application to a Real Case of Cyberbullying," 2015, 419–28, https://doi.org/10.1093/jigpal/jzv048.
[33] D Denning and W Baugh, "HIDING CRIMES IN CYBERSPACE," *Information, Communication & Society* 2 (1999): 251–76, https://doi.org/10.1080/136911899359583.

dalam menangani bukti digital dalam kasus deepfake adalah kompleksitas dalam pengumpulan dan verifikasi bukti tersebut. Hal ini disebabkan oleh kesulitan dalam membedakan antara media asli dan yang telah dimanipulasi, serta kurangnya kerangka hukum yang memadai untuk mengatur penggunaan bukti digital dalam konteks ini. Selain itu, teknologi *deepfake* yang terus berkembang menambah kesulitan dalam mendeteksi dan mengautentikasi bukti digital, yang dapat mengancam integritas bukti dalam proses peradilan.[34]

Pengumpulan bukti forensik digital dalam kasus *deepfake* pornografi anak menghadapi berbagai tantangan yang signifikan. Salah satu kesulitan utama adalah volume data yang sangat besar yang harus dikelola oleh para ahli forensik digital. Hal ini dapat menyebabkan kendala waktu dan efisiensi dalam proses investigasi.[35]

Pembuktian forensik digital dalam kasus *deepfake* pornografi anak memerlukan pendekatan yang inovatif dan teknologi yang canggih. Penggunaan metode pembelajaran mendalam (*deep learning*) telah diusulkan untuk mendeteksi konten pornografi anak dengan menganalisis log teks, nama file, dan situs seluler.[36] Namun, meskipun teknologi ini menjanjikan, masih ada batasan dalam alat forensik saat ini yang perlu diatasi untuk meningkatkan akurasi dan keandalan deteksi *deepfake*. Pengembangan teknologi deteksi yang lebih maju dan otomatis sangat penting untuk mengatasi tantangan ini dan memastikan bahwa bukti yang dihasilkan dapat digunakan secara efektif dalam proses hukum.

D. PENUTUP

1. KESIMPULAN

Teknologi *deepfake* telah membawa tantangan besar dalam penegakan hukum, khususnya terkait kasus deepfake pornografi anak di Indonesia. Meskipun regulasi seperti UU Pornografi dan UU ITE telah mengatur berbagai kejahatan digital, belum ada aturan spesifik yang mencakup teknologi *deepfake*. Tantangan utama dalam penanganan kasus ini meliputi keterbatasan teknologi di pihak penegak hukum, kesulitan dalam mengidentifikasi pelaku, serta pembuktian bukti digital yang valid di pengadilan. Hal ini menunjukkan bahwa kerangka hukum yang ada belum sepenuhnya mampu mengakomodasi perkembangan teknologi dan kompleksitas kejahatan berbasis AI.

Untuk mengatasi masalah ini, pembaruan regulasi yang secara khusus mengatur kejahatan berbasis teknologi deepfake sangat diperlukan. Selain itu, peningkatan kapasitas teknis penegak hukum melalui pelatihan teknologi dan pengadaan alat pendukung menjadi langkah strategis yang harus diambil. Kampanye literasi digital juga penting untuk meningkatkan kesadaran masyarakat terhadap risiko teknologi ini. Di sisi lain, kerja sama internasional diperlukan untuk menghadapi sifat global dari kejahatan *deepfake*, sehingga upaya penegakan hukum dapat dilakukan secara lebih efektif dan komprehensif.

---

[34] Ebrima Hydara, Masato Kikuchi, and Tadachika Ozono, "Empirical Assessment of Deepfake Detection: Advancing Judicial Evidence Verification Through Artificial Intelligence," *IEEE Access* 12 (2024): 151188–203, https://doi.org/10.1109/ACCESS.2024.3480320.

[35] Christos Liambas and Athanasios Manios, "Pornography Image Detection in Digital Forensics," *2023 8th International Conference on Frontiers of Signal Processing (ICFSP)*, 2023, 88–92, https://doi.org/10.1109/ICFSP59764.2023.10372879.

[36] Farkhund Iqbal et al., "A Study of Detecting Child Pornography on Smart Phone," 2017, 373–84, https://doi.org/10.1007/978-3-319-65521-5_32.

2. **SARAN**
   a. Pembaruan Regulasi: Pemerintah perlu segera melakukan revisi atau pembaruan terhadap peraturan yang ada untuk mencakup secara spesifik kejahatan berbasis teknologi deepfake, termasuk yang terkait dengan eksploitasi anak.
   b. Pelatihan Penegak Hukum: Kapasitas teknologi para penegak hukum harus ditingkatkan melalui pelatihan dan pengadaan alat-alat pendukung untuk identifikasi dan investigasi kejahatan berbasis deepfake.
   c. Kampanye Literasi Digital: Pemerintah, bersama dengan lembaga terkait, perlu mengedukasi masyarakat tentang risiko teknologi deepfake dan cara melindungi diri dari eksploitasi digital.
   d. Peningkatan Infrastruktur Teknologi: Investasi dalam infrastruktur teknologi canggih perlu dilakukan untuk membantu penegak hukum menangani bukti digital secara efektif.

DAFTAR PUSTAKA

Ahmad, Dwi Nurfauziah, and Latifatul Hidayati. "LAW ENFORCEMENT AGAINST CRIMINAL ACTORS OF CHILD PORNOGRAPHY THROUGH SOCIAL MEDIA." *JHR (Jurnal Hukum Replik)*, 2021. https://doi.org/10.31000/JHR.V9I1.4120.

Algamar, Muhammad Deckri, and Aliya Ilysia Irfana Ampri. "Hak Untuk Dilupakan: Penghapusan Jejak Digital Sebagai Perlindungan Selebriti Anak Dari Bahaya Deepfake." *JURNAL YUSTIKA: MEDIA HUKUM DAN KEADILAN*, 2022. https://doi.org/10.24123/yustika.v25i01.5091.

Armstrong, H, and Patrick Forde. "Internet Anonymity Practices in Computer Crime." *Inf. Manag. Comput. Secur.* 11 (2003): 209–15. https://doi.org/10.1108/09685220310500117.

Arumawan, Dicky Putra, and S Iksan. "Implementasi Penegakan Sanksi Pidana Dalam Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi (Studi Kasus Di Wilayah Hukum Pengadilan Negeri Boyolali)," 2016. https://consensus.app/papers/implementasi-penegakan-sanksi-pidana-dalam-undangundang-arumawan-iksan/36967d0de13554548bba83cef208b23c/.

Coccomini, D. "Deepfake Detection: Challenges and Solutions," 2023, 688–89. https://consensus.app/papers/deepfake-detection-challenges-and-solutions-coccomini/e1b9d4babc1f50799ba4247904e10509/.

Denning, D, and W Baugh. "HIDING CRIMES IN CYBERSPACE." *Information, Communication & Society* 2 (1999): 251–76. https://doi.org/10.1080/136911899359583.

Efremova, Marina, and E Russkevich. "Deepfake And Criminal Law." *Bulletin of the Kazan Law Institute of MIA Russia*, 2024. https://doi.org/10.37973/vestnikkui-2024-56-13.

Fatmawati, and Raihana Raihana. "Analisis Yuridis Terhadap Artificial Intelligence Pada Tindak Pidana Penyebaran Malware Di Indonesia." *INNOVATIVE Journal Of Social Science Research* 3 (June 18, 2023): 12190–201.

Galán-García, Patxi, José Gaviria De La Puerta, Carlos Laorden, Igor Santos, and P Bringas. "Supervised Machine Learning for the Detection of Troll Profiles in Twitter Social Network: Application to a Real Case of Cyberbullying," 2015, 419–28. https://doi.org/10.1093/jigpal/jzv048.

Gunawan, Ratu Agung Dewangga Arinatha, Nyoman Gede Sugiartha, and Ni Made Sukaryati Karma. "Penyebaran Iklan Pada Media Elektronik Yang Memuat Konten Pornografi." *Jurnal Interpretasi Hukum*, 2021. https://doi.org/10.22225/juinhum.2.2.3421.261-267.

Hanif, Saiyad Mahmmadakram, and Vivek Dave. "Deepfakes Technology Using AI." *International Journal of Scientific Research in Science, Engineering and Technology*, 2022. https://doi.org/10.32628/ijsrset229522.

Hung, Tzu-Wei, and Chun-Ping Yen. "On the Person-Based Predictive Policing of AI." *Ethics and Information Technology* 23 (2020): 165–76. https://doi.org/10.1007/s10676-020-09539-x.

Hydara, Ebrima, Masato Kikuchi, and Tadachika Ozono. "Empirical Assessment of Deepfake Detection: Advancing Judicial Evidence Verification Through Artificial Intelligence." *IEEE Access* 12 (2024): 151188–203. https://doi.org/10.1109/ACCESS.2024.3480320.

Iqbal, Farkhund, Andrew Marrington, P Hung, Jing-Jie Lin, Guan-Pu Pan, Shih-Chia Huang, and Benjamin Yankson. "A Study of Detecting Child Pornography on Smart Phone," 2017, 373–84. https://doi.org/10.1007/978-3-319-65521-5_32.

Karasavva, Vasileia, and Aalia Noorbhai. "The Real Threat of Deepfake Pornography: A Review of Canadian Policy." *Cyberpsychology, Behavior and Social Networking* 24 3 (2021): 203–9. https://doi.org/10.1089/cyber.2020.0272.

Kiliç, Büşra, and Mehmet Emin Kahraman. "Current Usage Areas of Deepfake Applications with Artificial Intelligence Technology." *İletişim ve Toplum Araştırmaları Dergisi*, 2023. https://doi.org/10.59534/jcss.1358318.

Kumar, Manoj, Praveen Kumar Rai, and Pankaj Kumar. "A Novel Approach for Detecting Deepfake Face Using Machine Learning Algorithms." *2024 2nd International Conference on Disruptive Technologies (ICDT)*, 2024, 1588–92. https://doi.org/10.1109/ICDT61202.2024.10489036.

Liambas, Christos, and Athanasios Manios. "Pornography Image Detection in Digital Forensics." *2023 8th International Conference on Frontiers of Signal Processing (ICFSP)*, 2023, 88–92. https://doi.org/10.1109/ICFSP59764.2023.10372879.

Mrvić-Petrović, Nataša. "Criminal Law Approach to Regulating Non-Consensual Pornographic Deepfake." *Bezbednost, Beograd*, 2024. https://doi.org/10.5937/bezbednost2402005p.

Murdan, M. "Membaca Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi Dari Perspektif Sosiologi Hukum." *Indonesian Journal of Shariah and Justice*, 2021. https://doi.org/10.46339/ijsj.v1i1.5.

Octarina, Nynda Fatmawati, and M Hasan. "The Urgency of Regulating Access to Pornography Content in Law No. 44 of 2008 Concerning Pornography." *International Journal of Science and Society*, 2023. https://doi.org/10.54783/ijsoc.v5i1.643.

Panda, Jayanta Kumar, and Rajnandini Panigrahy. "Unmasking Deception In The Age Of Artificial Intelligence: A Comprehensive Analysis Of Indian Celebrity's Deepfakes News." *ShodhKosh: Journal of Visual and Performing Arts*, 2023. https://doi.org/10.29121/shodhkosh.v4.i2.2023.2268.

Purwono, Agus, M Zamroni, Hardi Anugrah Santoso, Fajar Rachmad, and Dwi Miarsa. "IMPLICATIONS AND CONSIDERATIONS OF THE NEW ELECTRONIC INFORMATION AND TRANSACTION LAW." *ANAYASA : Journal of Legal Studies*, 2024. https://doi.org/10.61397/ays.v1i2.242.

Rachmadie, D T. "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016." *Jurnal Hukum Pidana Dan Penanggulangan Kejahatan* 9, no. 2 (2016): 128–36. https://jurnal.uns.ac.id/recidive/article/view/47400.

Rahmat, Z. "Localism Principle in the Formulation of Indonesian Regulations on Pornography" 12 (2020): 167–77. https://doi.org/10.18196/jkm.122045.

Rana, M, M Nobi, B Murali, and A Sung. "Deepfake Detection: A Systematic Literature Review." *IEEE Access* 10 (2022): 25494–513. https://doi.org/10.1109/access.2022.3154404.

Saifuddin Anwar. *Metode Penelitian*. Cet. III. Yogyakarta: Pustaka Pelajar Offset, 2016.

Shahzad, H, F Rustam, E Flores, Juan Luís Vidal Mazón, I Díez, and Imran Ashraf. "A Review of Image Processing Techniques for Deepfakes." *Sensors (Basel, Switzerland)* 22 (2022). https://doi.org/10.3390/s22124556.

Singh, Hardeep, Kamaljeet Kaur, Fakira Mohan Nahak, Sandeep Kumar Singh, and Sandeep Kumar. "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.

Sousa-Gomes, Valéria, Beatriz Abreu, D Moreira, Amaia Del Campo, D Moreira, and Marisalva Fávero. "Psychological Intervention and Treatment Programs for Adult Victims of Child Sexual Abuse: A Systematic Review." *Psychological Trauma : Theory, Research, Practice and Policy*, 2022. https://doi.org/10.1037/tra0001389.

Supriya, Shree, Riddhi Arya, and Saket Kumar Roy. "Investigating the Evolving Landscape of Deepfake Technology: Generative AI's Role in It's Generation and Detection." *International Research Journal on Advanced Engineering Hub (IRJAEH)*, 2024. https://doi.org/10.47392/irjaeh.2024.0206.

Timothy Adrianus P Gultom, Diah Pawestri Maharani, Afrizal Mukti Wibowo. "Analisis Yuridis Penggunaan Artificial Intelligence Yang Menjalankan Fungsi Legal Audit Dalam Regulatory Compliance System Di Indonesia: The Juridical Analysis of the Use of Artificial Intelligence Performing Legal Audit Function in Regulatory Compliance." *Brawijaya Law Student Journal*, March 18, 2024. https://hukum.studentjournal.ub.ac.id/index.php/hukum/article/view/5809.

Verdoliva, L. "Media Forensics and DeepFakes: An Overview." *IEEE Journal of Selected Topics in Signal Processing* 14 (2020): 910–32. https://doi.org/10.1109/JSTSP.2020.3002101.

Wibisono, Muhammad Iqbal, and Bahrul Fawaid. "Larangan Pornografi Dalam Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi (Perspektif Asas Legalitas)." *QISTIE*, 2022. https://doi.org/10.31942/jqi.v14i2.6084.

Yunarti, Sri, Syakir, Ashabul Fadli, and Mami Nofrianti. "Internasional Conference on Humanity, Law and Sharia (ICHLaSh). November 14-15. 2018 Reconstruction on Sharia Sciences in Facing Contemporary Law Problematics/97 EXAMINATION OF CONSTITUTIONALITY OF CHILD PROTECTION LAW IN FIQH," 2020. https://consensus.app/papers/internasional-conference-on-humanity-law-and-sharia-yunarti-syakir/7134f16f511955a9abc90f866defeb7a/.

Peraturan Perundang-Undangan :

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi.