



Pengaturan Hukum dalam Penanggulangan *Deepfake Artificial Intelligence* (AI) terhadap Anak sebagai Korban Kejahatan Siber di Indonesia

Putu Nadya Tasya Putri¹, Anak Agung Ayu Ngurah Tini Rusmini Gorda²

¹Fakultas Hukum Universitas Pendidikan Nasional, E-mail: ms.nasyap@gmail.com

²Fakultas Hukum Universitas Pendidikan Nasional, E-mail: tinirusmini@undiknas.ac.id.

Info Artikel

Masuk: 9 Juli 2025

Diterima: 30 September 2025

Terbit: 30 September 2025

Keywords:

The Legal Framework; Child Protection; Artificial Intelligence; Deepfake; Cyber Violence.

Kata kunci:

Pengaturan Hukum;
Perlindungan Anak;
Kecerdasan Buatan; Deepfake;
Kejahatan Siber.

Corresponding Author:

Putu Nadya Tasya Putri, E-mail: ms.nasyap@gmail.com

DOI:

10.24843/JMHU.2025.v14.i03.p09

Abstract

This research analyzes the development of Artificial Intelligence (AI) technology, particularly through Deepfake, which has given rise to a new form of cyber sexual violence against children in the form of AI-generated child sexual abuse material (AI-CSAM). Although such content does not involve children physically, it still constitutes sexual exploitation in substance. This issue has not yet been specifically regulated under Indonesian law, resulting in a legal vacuum (rechtsvacuum). This study seeks to examine how Indonesian law regulates Deepfake AI-related crimes involving children, and the urgency of legal reform in addressing the legal vacuum concerning perpetrators of AI-CSAM-related offenses. This research employs normative legal methods using a statute approach and comparative approach. The results show that the current legal framework in Indonesia is insufficient to effectively address AI-CSAM content. Legal frameworks from other jurisdictions, such as the European Union and the United Kingdom, may serve as valuable references for national legal reform. Therefore, it is recommended that a specific regulation be formulated to govern AI-based Deepfake content as a form of sexual violence against children.

Abstrak

Penelitian ini menganalisis Perkembangan teknologi kecerdasan buatan (Artificial Intelligence/AI), khususnya melalui Deepfake, telah menimbulkan bentuk baru kekerasan seksual siber terhadap anak dalam bentuk AI-generated child sexual abuse material (AI-CSAM). Meskipun konten tersebut tidak melibatkan anak secara fisik, substansinya tetap mengandung eksploitasi seksual. Hal tersebut belum diatur belum secara khusus di Indonesia, sehingga menimbulkan kekosongan hukum (rechtsvacuum). Penelitian ini akan membahas mengenai Bagaimana pengaturan hukum di Indonesia terhadap kejahatan Deepfake AI terhadap anak dan Bagaimana urgensi pembaruan hukum dalam mengatasi kekosongan hukum terkait pelaku kejahatan dengan AI-CASM. Penelitian ini menggunakan penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan perbandingan Hasil penelitian menunjukkan bahwa peraturan hukum di Indonesia belum memadai dalam menjangkau konten AI-CSAM.

Pengaturan dari negara lain, seperti Uni Eropa dan Inggris, dapat menjadi referensi dalam pembaruan hukum nasional. Oleh karena itu, disarankan agar segera dirumuskan regulasi khusus yang mengatur konten Deepfake berbasis AI sebagai bagian dari kekerasan seksual terhadap anak.

I. Pendahuluan

Perkembangan teknologi informasi dan komunikasi sudah berkembang secara signifikan selama dua dekade terakhir, terutama pada ranah kecerdasan buatan atau *Artificial Intelligence* (AI).¹ AI tidak lagi sekadar gagasan abstrak dalam dunia akademik atau laboratorium teknologi, tetapi telah menjadi bagian integral dari kehidupan manusia modern. Mulai dari sistem navigasi, perangkat lunak prediktif, algoritma media sosial, hingga pengenalan wajah, AI memainkan peran signifikan dalam membantu pengambilan keputusan dan peningkatan efisiensi di berbagai sektor. Peran AI dalam kehidupan sehari-hari terus berkembang, bahkan telah merambah ranah yang lebih kompleks, seperti penciptaan konten digital yang menyerupai realitas kehidupan manusia yang sering kita lihat pada sosial media.

Salah satu inovasi AI yang paling menonjol dan kontroversial adalah *Deepfake*, yakni teknologi yang menggunakan *machine learning* dan *generative adversarial networks* (GANs) untuk memanipulasi gambar, suara, atau video seseorang secara realistis.² *Deepfake* memungkinkan penciptaan representasi visual atau audio dari individu tertentu yang seolah-olah melakukan suatu tindakan atau mengucapkan pernyataan, padahal kenyataannya tidak demikian. Teknologi ini awalnya dikembangkan untuk tujuan positif, seperti pelestarian budaya, rekonstruksi sejarah, simulasi medis, dan industri hiburan, termasuk penggantian aktor atau pelatihan berbasis virtual.

Namun demikian, potensi manfaat *Deepfake* diimbangi oleh risiko penyalahgunaan yang tinggi. Dalam beberapa tahun terakhir, penyalahgunaan *Deepfake* telah menjadi sorotan global, khususnya dalam bentuk pembuatan konten pornografi non-konsensual, penyebaran disinformasi politik, dan identity theft. Sebuah laporan dari Sensity AI (2020) menunjukkan bahwa lebih dari 90% konten *Deepfake* yang beredar di internet merupakan pornografi, dan sebagian besar melibatkan perempuan sebagai korban.³ Lebih memprihatinkan lagi, teknologi ini kini mulai digunakan untuk menciptakan konten seksual yang menampilkan anak-anak, baik yang menyerupai korban nyata maupun yang sepenuhnya dihasilkan secara artifisial. Fenomena ini dikenal sebagai *AI-generated Child Sexual Abuse Material* (AI-CSAM).

¹ Dewi Tresnawati et al., "Artificial Intelligence Serta Singularitas Suatu Kekeliruan Atau Tantangan," *Jurnal Algoritma* 19, no. 1 (2022): 181-88. <https://doi.org/10.33364/algoritma/v.19-1.1028>

² Dwi Fitri et al., "*Deepfake* Dan Krisis Kepercayaan: Analisis Hukum Terhadap Penyebaran Konten Palsu Di Media Sosial," *Jurnal Intelek Insan Cendikia* 2, no. 6 (2025): 11556-68.

³ Alexander Diel et al., "Human Performance in Detecting *Deepfakes*: A Systematic Review and Meta-Analysis of 56 Papers," *Computers in Human Behavior Reports* 16 (2024): 100538. <https://doi.org/10.1016/j.chbr.2024.100538>

AI-CSAM merupakan bentuk baru dari kekerasan seksual siber yang sangat kompleks. Meskipun tidak melibatkan anak secara fisik dalam proses pembuatan konten, substansi dari konten tersebut tetap merupakan eksploitasi seksual, selain itu AI-CASM sangat berbahaya apabila dilihat anak-anak. Representasi visual anak dalam posisi atau tindakan seksual, meskipun sepenuhnya hasil rekayasa digital, tetap dapat menyebabkan kerugian psikologis dan sosial, serta mendorong normalisasi pornografi anak. Konten semacam ini juga berpotensi dikomersialisasi melalui forum-forum ilegal di dunia maya, memperluas jangkauan pasar eksploitasi anak secara digital.⁴

Menurut data dari Internet Watch Foundation (IWF) tahun 2022, ditemukan bahwa lebih dari 7.000 konten pornografi anak di dunia maya dihasilkan menggunakan teknologi *Deepfake*, dan jumlah tersebut meningkat lebih dari 250% dibandingkan tahun sebelumnya.⁵ Temuan ini mengindikasikan tren yang mengkhawatirkan di mana teknologi digital canggih digunakan untuk memperkuat industri eksploitasi seksual anak secara global, termasuk di kawasan Asia Tenggara. Dalam konteks ini, Indonesia yang memiliki jumlah pengguna internet aktif terbesar keempat di dunia menjadi sangat rentan terhadap penyebaran konten AI-CSAM. Sayangnya, sampai sekarang belum terdapat informasi resmi yang mencatat jumlah penyebaran konten *Deepfake* bermuatan pornografi anak di Indonesia secara khusus, yang menunjukkan kurangnya perhatian dan pengawasan terhadap bentuk kejahatan digital ini.

Anak sebagai subjek hukum yang lemah dan rentan memerlukan perlindungan hukum yang kuat dan komprehensif. Perlindungan kepada anak dari seluruh wujud kekerasan, termasuk kekerasan seksual berbasis teknologi, merupakan kewajiban konstitusional negara seperti tercantum pada Pasal 28B ayat (2) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Di tingkat undang-undang, pengaturan terkait perlindungan anak terdapat dalam Undang-Undang Nomor 35 Tahun 2014 tentang Perlindungan Anak, serta Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Namun, dalam konteks perkembangan AI dan teknologi *Deepfake*, instrumen hukum nasional belum cukup responsif. Kedua undang-undang tersebut tidak secara eksplisit mengatur bentuk kejahatan digital yang bersumber dari kecerdasan buatan, khususnya yang menyangkut anak sebagai objek eksploitasi seksual. Dalam UU ITE, pasal-pasal terkait distribusi informasi bermuatan pornografi belum memperhitungkan kemungkinan bahwa konten tersebut sepenuhnya dihasilkan oleh sistem non-manusia. Sementara itu, UU Perlindungan Anak lebih berfokus pada bentuk-bentuk kekerasan konvensional, baik fisik maupun psikis, yang sulit menjangkau konten artifisial yang menyerupai pornografi anak.

Selain UU ITE dan UU Perlindungan Anak, penting pula memperhatikan Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, terutama dalam konteks konten seksual yang menyangkut anak. Pada Pasal 1 angka 1, dinyatakan bahwa pornografi mencakup gambar, suara, tulisan, gerak tubuh, dan bentuk komunikasi lainnya yang

⁴ Amy Trivison, "Understanding the Line Between Art and Abuse: How Generative AI Changes the Landscape of Child Sexual Abuse Materials," *Catholic University Journal of Law and Technology* 33, no. 1 (2024): 87-114.

⁵ Internet Watch Foundation, "IWF Annual Report 2022," 2022, <https://www.iwf.org.uk/about-us/who-we-are/annual-report-2022/>.

mengandung muatan seksual. Sementara itu, Pasal 4 ayat (1) huruf f secara tegas melarang pembuatan, penyebaran, dan kepemilikan pornografi anak, tanpa menjelaskan secara rinci apakah konten tersebut harus berbasis nyata atau dapat berupa rekayasa digital. Dengan demikian, secara konstruktif, ketentuan dalam UU Pornografi dapat ditafsirkan inklusif terhadap konten *Deepfake* berbasis AI. Namun, hingga kini belum ada peraturan turunan atau yurisprudensi yang menegaskan bahwa *AI-generated content* termasuk dalam kategori yang dimaksud oleh undang-undang tersebut. Hal ini menunjukkan bahwa sekalipun norma telah tersedia, kekosongan dalam penafsiran dan pelaksanaan hukum tetap menjadi hambatan dalam perlindungan anak dari eksploitasi seksual digital.

Kondisi ini menimbulkan kekosongan hukum (*rechtsvacuum*) dalam sistem hukum nasional. Kejahatan baru berbasis AI tidak dapat dikenai sanksi pidana secara efektif karena tidak adanya rumusan delik yang sesuai. Akibatnya, pelaku penyebaran atau pencipta konten AI-CSAM dapat lolos dari jerat hukum, sementara korban, meskipun tidak terlibat langsung, tetap mengalami kerugian psikologis, sosial, dan hukum. Hal ini juga menimbulkan ketidakpastian hukum (*rechtsonzekerheid*) dan menghambat pemenuhan hak atas perlindungan hukum (*rechtsbescherming*) bagi anak.

Sebaliknya, beberapa negara di dunia telah mulai merespons fenomena ini melalui kebijakan dan peraturan yang progresif. Uni Eropa, misalnya, melalui *Artificial Intelligence Act*, telah menetapkan klasifikasi risiko untuk penggunaan AI, termasuk larangan terhadap penggunaan AI untuk eksploitasi seksual anak. Inggris mengesahkan *Online Safety Act 2023*, yang memberikan kewenangan kepada penegak hukum untuk menindak *platform* digital yang mengizinkan penyebaran konten *Deepfake* pornografi anak.⁶ Di Amerika Serikat, sejumlah negara bagian telah mengatur larangan *Deepfake* pornografi dalam kerangka hukum pidana, meskipun belum diatur secara federal. Negara seperti Kanada juga telah merilis pedoman kebijakan nasional mengenai perlindungan anak terhadap AI generatif melalui kerja sama antara lembaga perlindungan anak dan lembaga pengembangan teknologi.

Langkah-langkah yang diambil oleh negara-negara tersebut menunjukkan bahwa peraturan yang adaptif dan antisipatif terhadap perkembangan teknologi mutakhir sangat mungkin untuk dirancang dan diterapkan. Dalam konteks Indonesia, keterlambatan dalam merespons fenomena ini bukan hanya berdampak pada kekosongan hukum semata, tetapi juga mencerminkan kelemahan dalam mekanisme perlindungan anak secara menyeluruh. Oleh karena itu, diperlukan pembaruan hukum yang tidak hanya bersifat reaktif, tetapi juga mampu menjadi dasar normatif dalam menghadapi tantangan digital secara sistemik.

Melihat ketertinggalan peraturan di Indonesia dibandingkan dengan praktik-praktik negara yang disebutkan di atas, sangat penting untuk segera melakukan pembaruan hukum nasional guna mengisi kekosongan tersebut. Karenanya, penelitian ini ingin membahas serta menganalisis kekosongan hukum dalam penanggulangan kejahatan *Deepfake* AI terhadap anak sebagai bentuk kekerasan seksual siber, serta menawarkan arah reformulasi hukum nasional yang dapat dijadikan acuan dalam merespons tantangan teknologi digital masa kini.

⁶ Agus Wibowo and Sri Yulianingsih, "Hukum Teknologi Informasi," Penerbit Yayasan Prima Agus Teknik, 2025.

Terkait dengan fokus penelitian ini, sejumlah artikel jurnal dan karya ilmiah sebelumnya telah membahas fenomena *Deepfake* dan kecerdasan buatan (AI). Namun, sebagian besar kajian tersebut masih bersifat umum dan tidak secara spesifik menyoroti persoalan eksploitasi seksual anak melalui konten *AI-generated* (AI-CSAM). Penelitian oleh Rizki Fahmi dan Rahmad Hidayat, misalnya, dalam artikel berjudul "*Tinjauan Yuridis Terhadap Penggunaan Deepfake dalam Perspektif Hukum Pidana*" lebih menekankan pada aspek pencemaran nama baik dan pemalsuan identitas, tetapi belum menyentuh kerentanan anak sebagai korban kekerasan seksual berbasis teknologi. Demikian pula, tulisan Wahyudi dalam "*Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI*" lebih menitikberatkan pada penggunaan *Deepfake* dalam konteks disinformasi politik. Sementara itu, kajian Loso Judjianto dan Rabith Madah Khulaili Harsya dalam artikel "*Etika dan Hukum dalam Penggunaan Artificial Intelligence terhadap Privasi Digital di Indonesia*" berfokus pada isu privasi dan perlindungan data pribadi. Dengan demikian, penelitian ini berbeda karena secara khusus mengarahkan analisis pada implikasi hukum pidana terhadap penyalahgunaan *Deepfake AI* untuk menghasilkan materi kekerasan seksual anak (AI-CSAM), suatu topik yang belum mendapatkan perhatian memadai dalam literatur hukum di Indonesia.⁷

Tujuan tulisan ini menganalisis tentang penegakan hukum tindak pidana pencucian uang menggunakan *cryptocurrency* dan terkait pengaturan *cryptocurrency* sebagai objek pencucian uang di Indonesia. Latar belakang yang sudah diterangkan tersebut, harus kita pahami serta dianalisis mendalam kajian berkenaan bagaimana pengaturan hukum positif Indonesia terhadap kejahatan *Deepfake AI* yang menyasar anak sebagai korban kekerasan seksual siber dan bagaimana urgensi dan arah pembaruan hukum nasional dalam mengatasi kekosongan hukum (*rechtsvacuum*) terhadap konten *AI-generated child sexual abuse material* (AI-CSAM).

2. Metode Penelitian

Penelitian hukum ini memakai metode penelitian hukum normatif yang berfokus pada bahan pustaka dalam menjawab rumusan masalah. Pendekatan yang dipakai adalah pendekatan perundang-undangan dan pendekatan komparatif. Pendekatan undang-undang mengkaji pengaturan hukum positif Indonesia terhadap kejahatan *Deepfake AI* yang menyasar anak sebagai korban kekerasan seksual siber. Selain itu, pendekatan komparatif dilaksanakan melalui membandingkan peraturan perundang-undangan di sebuah negara dengan peraturan perundang-undangan di negara lain. Pendekatan komparatif dalam penelitian ini akan mengkaji peraturan dan penegakan hukum terkait kejahatan *Deepfake AI* yang menyasar anak di Indonesia yang belum cukup mumpuni dibandingkan dengan peraturan di negara Inggris yang lebih progresif dalam menangani hal tersebut. Penelitian ini menggunakan analisis deskriptif-analitis yaitu dengan menggunakan tulisan untuk menguraikan masalah berdasarkan data yang ada kemudian menganalisisnya untuk menarik kesimpulan. Ini menganalisis topik semantik dari publikasi jurnal terkemuka untuk menjawab pertanyaan-pertanyaan ini.⁸

⁷ Loso Judjianto and Rabith Madah Khulaili Harsya, "Etika Dan Hukum Dalam Penggunaan Artificial Intelligence Terhadap Privasi Digital Di Indonesia," *Sanskara Hukum Dan HAM* 3, no. 03 (2025): 141–49.

⁸ Peter Mahmud Marzuki, *Penelitian Hukum Edisi Revisi* (Jakarta: Kencana, 2017).

3. Hasil dan Pembahasan

3.1 Pengaturan Hukum Positif Indonesia terhadap Kejahatan *Deepfake* AI yang Menyasar Anak

Fenomena kejahatan seksual siber terhadap anak melalui teknologi *Deepfake* AI merupakan isu hukum kontemporer yang mendesak untuk dianalisis secara sistematis. Teknologi *Deepfake* memungkinkan penciptaan citra dan video artifisial yang meniru secara persis wajah dan tubuh seseorang, termasuk anak, dalam konteks yang bersifat seksual. Ini membuka ruang eksploitasi baru terhadap anak meskipun anak tidak terlibat secara fisik, karena citra digital yang disebarluaskan tetap dapat menimbulkan trauma psikologis, kerusakan reputasi, dan stigma sosial.⁹

Penggunaan *Deepfake* AI sebagai konten yang dapat menciptakan atau membuat muatan pornografi khususnya pornografi yang melibatkan anak dianggap sebagai tindak pidana kesusilaan, seperti yang tercantum pada Pasal 281 KUHP, yang singkatnya mengemukakan : bagi mereka yang dengan sengaja secara dan secara terbuka melakukan pelanggaran kesusilaan maka dapat dijatuhi tindak pidana penjara paling lama 2 (dua) tahun 8 (delapan) bulan atau denda paling banyak Rp4.500.000. Namun saat ini, masih belum terdapat kejelasan mengenai bagaimana bentuk pelanggaran di dalam Pasal 281 tersebut. Menurut hemat penulis, penyalahgunaan *Deepfake* AI sebagai kecerdasan buatan yang dapat memuat konten pornografi terhadap anak adalah pelanggaran kesusilaan yang dapat membuat anak sebagai korban, baik korban langsung maupun tidak langsung. Anak sebagai korban langsung yakni anak yang dimanipulasi wajahnya dalam muatan konten pornografi, sedangkan anak sebagai korban tidak langsung yakni anak-anak yang melihat atau menonton konten pornografi *Deepfake* AI itu, yang secara tidak langsung menggerus moral dan mental anak-anak.¹⁰

Pengaturan terhadap kekerasan seksual berbasis teknologi di Indonesia masih sangat terbatas. Dalam UU ITE khususnya, Pasal 27 ayat (1) UU ITE mengatur larangan distribusi informasi elektronik yang bermuatan kesusilaan, tetapi pasal ini lebih bersifat umum dan tidak menjelaskan batasan serta klasifikasi konten buatan AI.¹¹ Tidak adanya penjabaran dalam penjelasan pasal atau yurisprudensi yang mendukung interpretasi bahwa konten AI termasuk dalam cakupan pasal tersebut, memperlemah efektivitas penegakan hukumnya. Selain itu, konsep kesusilaan dalam UU ITE sering kali bergantung pada subjektivitas aparat penegak hukum, yang memperbesar kemungkinan multitafsir dalam penerapan.

Pengaturan selanjutnya terdapat pada Undang-Undang Nomor 35 Tahun 2014 tentang Perlindungan Anak (UU Perlindungan Anak). UU Perlindungan Anak secara eksplisit melarang perlakuan terhadap anak sebagai objek pornografi seperti

⁹ Fuadi Isnawan, "Deepfake Pornography: How Criminal Liability of Perpetrators in the Indonesian Criminal Law Framework," *Jurnal Magister Hukum Udayana*, 2024, <https://doi.org/10.24843/JMHU.2024.v13.i03.p15>.

¹⁰ Rizgita Nurul Fauzyah, Putri Hafidati, and Sunarya Sunarya, "Perlindungan Hukum Terhadap Korban Tindak Pidana Pembuat Video Pornografi Palsu (*Deepfake* Porn) Berbasis Artificial Intelligence (AI) Di Indonesia," *Lex Veritatis* 3, no. 3 (2024): 74–88.

¹¹ Izil Hidayat Putra, "Perlindungan Hukum Terhadap Korban Penyalahgunaan Artificial Intelligence (AI) Berupa *Deepfake* Pornografi Menurut Peraturan Perundang-Undangan," *UNJA Journal of Legal Studies* 1, no. 2 (2024): 110–28.

tercantum pada Pasal 76D serta 76E. Akan tetapi, pasal-pasal tersebut belum memberikan ruang lingkup yang memadai terhadap konten yang sepenuhnya dihasilkan melalui algoritma kecerdasan buatan. Secara normatif, anak sebagai subjek hukum memiliki hak perlindungan hukum secara maksimal dari berbagai bentuk eksploitasi, tetapi hingga saat ini belum terdapat norma yang secara jelas memperluas makna "perlakuan sebagai objek pornografi" mencakup konten digital fiktif berbasis AI.¹²

UU Pornografi, sebagai salah satu instrumen hukum yang lebih spesifik, memang memberikan larangan eksplisit terhadap pembuatan dan penyebaran konten yang mengandung eksploitasi seksual anak (Pasal 4 ayat (1) huruf f). Namun, sama halnya dengan dua UU lainnya, pengaturan dalam UU ini belum secara tegas mencantumkan istilah atau ruang lingkup terhadap konten rekayasa digital. Tanpa interpretasi progresif atau pembaruan dalam bentuk peraturan pelaksana, norma tersebut belum cukup mampu menjangkau substansi kejahatan baru dalam bentuk *Deepfake*.

Penulis berpendapat saat ini dengan instrumen hukum yang ada, untuk menindak para pelaku penggunaan *Deepfake* AI dapat menggunakan ketentuan pasal 27 ayat (1) UU ITE, diatur larangan bagi setiap orang untuk dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan/atau membuat bisa diaksesnya informasi elektronik yang mempunyai muatan melanggar kesusilaan. Meskipun tidak menyebut istilah *Deepfake*, muatan pornografi hasil rekayasa digital dapat dikualifikasikan sebagai pelanggaran terhadap norma kesusilaan tersebut. Selain itu, dalam pembaruan melalui Pasal 16A, UU ITE menegaskan kewajiban penyelenggara sistem elektronik untuk melindungi anak dari konten atau aktivitas daring yang berpotensi merugikan, termasuk di dalamnya kejahatan digital berbasis manipulasi visual seperti *Deepfake*. UU Pornografi dapat digunakan sebagai dasar hukum untuk menjerat pelaku *Deepfake* pornografi anak. Pasal 4 ayat (2) undang-undang tersebut secara tegas melarang segala bentuk pornografi yang melibatkan anak sebagai objek, tanpa membedakan antara konten asli maupun hasil rekayasa digital. Ancaman pidana yang tercantum pada Pasal 29 UU Pornografi mencapai pidana penjara paling lama 12 tahun serta denda hingga enam miliar rupiah. Selanjutnya, UU Perlindungan anak, juga memberikan landasan hukum yang kuat. Pasal 76I melarang penyalahgunaan anak untuk kegiatan atau produk pornografi, sementara Pasal 82A yang ditambahkan melalui UU No. 17 Tahun 2016 mengatur sanksi pidana penjara minimal lima tahun serta maksimal dua puluh tahun bagi pelaku eksploitasi seksual terhadap anak, termasuk dalam bentuk simulasi digital.¹³

Ketiadaan pasal-pasal yang menyebutkan konten artifisial secara eksplisit menimbulkan celah hukum (*legal loophole*) yang signifikan. Dalam doktrin hukum pidana, dikenal asas legalitas (*nullum crimen sine lege* dan *nulla poena sine lege*) yang menyatakan bahwa tidak ada perbuatan dapat dipidana kecuali berlandaskan

¹² Kevin Amos Alexander Panjaitan, Prija Djatmika, and Alfons Zakaria, "Urgensi Pengaturan Hukum Terhadap Korban Tindak Pidana Pornografi *Deepfake* Di Indonesia," *Universitas Brawijaya*, 2025.

¹³ Meirza Aulia Chairani, Krista Yitawati, and Angga Pramodya Pradhana, "Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi *Deepfake*," *Jurnal Rechtsens* 13, no. 1 (2024), <https://doi.org/10.56013/rechtsens.v13i1.2668>.

ketetapan hukum yang sudah ada sebelumnya. Dalam konteks ini, apabila konten *Deepfake* AI tidak disebut secara eksplisit sebagai objek kejahatan, maka akan menyulitkan jaksa maupun hakim dalam menjerat pelaku berdasarkan hukum positif yang berlaku.¹⁴ Masalah lainnya adalah pendekatan hukum pidana nasional yang masih sangat bergantung pada konsepsi tradisional mengenai pelaku manusia (*natural person*). Teknologi AI tidak memiliki subjek hukum, namun dapat dimanfaatkan oleh manusia untuk menciptakan konten ilegal. Konsekuensinya, tidak adanya pengaturan terhadap peran teknologi dalam struktur tindak pidana berpotensi memperlemah sistem pembuktian dan unsur pertanggungjawaban pidana, terutama dalam konteks penyelidikan digital forensik.

Mireille Hildebrandt dalam teorinya yakni Teori *Legal Disruption*, menyatakan bahwa perkembangan teknologi digital telah mengguncang cara kerja norma hukum konvensional.¹⁵ Hukum tidak lagi cukup hanya sebagai refleksi sosial, tetapi harus menjadi instrumen yang mampu merespons inovasi secara adaptif dan berbasis risiko (*risk-based regulation*). Dalam konteks *Deepfake* AI, pendekatan ini menunjukkan bahwa hukum Indonesia belum siap menghadapi disrupsi digital yang kompleks, karena masih terpaku pada konstruksi hukum konvensional yang bersifat statis. Selain itu menurut *Techno Regulation Theory* yang dikembangkan oleh Lawrence Lessig. Ia menyatakan bahwa regulasi dalam era digital tidak hanya dijalankan oleh hukum, tetapi juga oleh arsitektur teknologi, norma sosial, dan pasar.¹⁶ Oleh sebab itu, kejahatan yang melibatkan *Deepfake* tidak bisa diselesaikan hanya dengan pendekatan hukum formal, tetapi juga harus mempertimbangkan bagaimana teknologi itu sendiri dapat dirancang untuk mencegah penyalahgunaan, misalnya melalui *watermarking* atau deteksi otomatis konten AI-CSAM.

Selain itu, dari perspektif Teori Perlindungan Hukum yang dikemukakan oleh Philipus M. Hadjon, hukum seharusnya hadir untuk memberikan perlindungan yang bersifat preventif dan represif terhadap hak-hak anak. Dalam konteks *Deepfake* AI, pengaturan yang kabur mengenai konten artifisial berimplikasi pada lemahnya perlindungan hukum, sehingga menuntut pembaruan norma agar anak benar-benar terlindungi dari eksploitasi berbasis teknologi. Di sisi lain, Teori Viktimologi juga penting digunakan untuk memahami kedudukan anak dalam kasus ini. Viktimologi menekankan bahwa korban tidak hanya dipahami sebagai pihak yang dirugikan secara fisik, tetapi juga psikologis dan sosial. Anak yang wajahnya dimanipulasi dalam konten pornografi *Deepfake* merupakan korban langsung, sementara anak-anak yang mengakses atau terpapar konten tersebut dapat disebut sebagai korban tidak langsung. Kerangka viktimologi ini memperluas pemahaman tentang dampak

¹⁴ Soetardi Tri Cahyono, Wina Erni, and Taufik Hidayat, "Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia," *Dame Journal of Law* 1, no. 1 (2025): 1-23.

¹⁵ Satria Muhammad Nur Lase, Aisyah Adinda, and Rizkia Diffa Yuliantika, "Kerangka Hukum Teknologi Blockchain Berdasarkan Hukum Siber Di Indonesia," *Padjadjaran Law Review* 9, no. 1 (2021).

¹⁶ Francesco De Vanna, "The Construction of a Normative Framework for Technology-Driven Innovations: A Legal Theory Perspective," *Use and Misuse of New Technologies: Contemporary Challenges in International and European Law*, 2019, 185-208.

kejahatan siber, sehingga mendorong perlunya formulasi norma pidana yang lebih progresif.

Berdasarkan ketentuan hukum yang berlaku di Indonesia, penyimpangan dalam pemanfaatan teknologi kecerdasan buatan, khususnya *Deepfake* yang mengandung unsur pornografi, belum mendapatkan pengaturan yang tegas dan terperinci. Meskipun demikian, sistem hukum positif Indonesia tetap menyediakan landasan normatif untuk menindak kasus semacam ini. Hasil analisis yuridis menunjukkan bahwa kemunculan teknologi *Deepfake* menimbulkan tantangan baru bagi sistem hukum nasional, mengingat peraturan yang ada belum secara eksplisit mengatur mengenai tindak pidana yang berkaitan dengan konten *Deepfake* berunsur pornografi. Oleh karena itu, sangat diperlukan peran aktif pemerintah dalam menyusun atau memperbarui regulasi yang secara khusus mengatur kejahatan *Deepfake* pornografi, guna menjamin adanya kepastian dan perlindungan hukum yang memadai.

Dengan kondisi tersebut, sangat diperlukan pembaruan hukum untuk menyesuaikan norma pidana dengan kompleksitas kejahatan modern yang melibatkan teknologi otonom. Pembaruan tersebut tidak hanya ditujukan untuk memperluas norma, tetapi juga menegaskan parameter pertanggungjawaban hukum pelaku yang memanfaatkan AI sebagai alat kejahatan. Norma pidana harus mampu melampaui pemahaman konvensional tentang kehadiran korban fisik dan menilai dampak hukum berdasarkan akibat hukum terhadap martabat dan perlindungan anak sebagai kelompok rentan.

3.2 Pembaruan hukum nasional dalam mengatasi kekosongan hukum (*rechtsvacuum*) terhadap konten AI-generated child sexual abuse material (AI-CSAM)

Pembahasan sebelumnya menganalisis mengenai sistem hukum nasional Indonesia belum memiliki instrumen normatif yang secara eksplisit mengatur kejahatan berbasis teknologi kecerdasan buatan, khususnya dalam konteks konten seksual terhadap anak yang dihasilkan oleh AI atau dikenal dengan istilah AI-generated child sexual abuse material (AI-CSAM). Undang-undang yang tersedia, yaitu UU ITE, UU Perlindungan Anak, dan UU Pornografi, belum mencantumkan ketentuan eksplisit mengenai konten digital fiktif hasil rekayasa algoritma atau manipulasi berbasis *Deepfake*. Akibatnya, terjadi kekosongan hukum (*rechtsvacuum*) yang berdampak pada ketidakpastian perlindungan hukum terhadap anak serta ketidakefektifan penegakan hukum terhadap pelaku.¹⁷

Kondisi ini dapat dijelaskan melalui Teori Kekosongan Hukum (*Rechtsvacuum Theory*) sebagaimana dikemukakan Hans Kelsen dan Utrecht, bahwa ketika norma positif tidak secara eksplisit mengatur fenomena baru, maka akan timbul ruang kosong dalam hukum yang menimbulkan ketidakpastian. Dalam konteks AI-CSAM, kekosongan hukum ini nyata karena tidak ada pasal yang secara tegas menyebut konten artifisial digital sebagai objek tindak pidana. Selain itu, Teori Perlindungan

¹⁷ Asri Gresmelian Eurike Hailtik and Wiwik Afifah, "Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia," *Asian Journal of Social and Humanities* 2, no. 4 (2023): 776–95.

Hukum dari Philipus M. Hadjon menegaskan bahwa hukum harus berfungsi melindungi hak-hak warga negara, terutama kelompok rentan. Anak sebagai kelompok yang memiliki hak atas perlindungan khusus justru menjadi korban eksploitasi dalam fenomena AI-CSAM. Ketiadaan pengaturan eksplisit memperlihatkan bahwa perlindungan hukum bagi anak masih sangat lemah.

Fenomena ini juga selaras dengan Teori Hukum Responsif dari Nonet dan Selznick yang menekankan bahwa hukum harus adaptif terhadap perubahan sosial. AI-CSAM merupakan bentuk kejahatan baru (*new emerging crimes*) yang menuntut regulasi adaptif. Jika hukum tetap kaku, maka ia kehilangan fungsinya sebagai instrumen keadilan.

Selain tidak adanya norma substantif yang komprehensif, kelemahan lain yang muncul ialah belum tersedianya kerangka prosedural yang jelas terkait pembuktian forensik terhadap konten AI, pertanggungjawaban pelaku yang menggunakan sistem otomatis, serta tidak adanya lembaga pengawas independen yang mengawasi distribusi konten berisiko tinggi di ranah digital. Untuk itu maka menurut penulis, Indonesia perlu melihat pengaturannya di negara lain khususnya Inggris dalam menangani fenomena AI CSAM yang menyasar anak.

Negara Inggris ialah salah satu negara yang paling progresif untuk merespons tantangan hukum yang ditimbulkan oleh teknologi *Deepfake*, khususnya dalam konteks perlindungan anak. Melalui *Online Safety Act 2023*,¹⁸ Inggris menegaskan kewajiban platform digital dan penyedia layanan internet untuk secara aktif mengidentifikasi, memblokir, dan melaporkan konten berbahaya termasuk konten *Deepfake* yang mengandung unsur seksual terhadap anak. Dalam konteks ini, kewajiban hukum tidak hanya dibebankan pada pelaku individu, tetapi juga pada penyedia layanan digital sebagai bagian dari sistem tanggung jawab hukum korporasi (*corporate liability*).¹⁹

Online Safety Act juga memperkenalkan konsep "*priority illegal content*", yakni klasifikasi konten yang wajib dihapus secara cepat oleh platform.²⁰ *AI-generated child sexual abuse material* termasuk dalam kategori ini. Selain itu, undang-undang tersebut memberikan kewenangan kepada Ofcom sebagai badan regulator independen untuk melakukan penyelidikan, menjatuhkan sanksi administratif, dan bahkan membatasi operasional *platform* yang melanggar kewajiban tersebut. Hal ini menandai adanya pergeseran paradigma dalam perlindungan anak, dari pendekatan hukum pidana semata ke arah pendekatan regulasi administratif dan preventif.

Selain pengaturan tersebut, Inggris juga memiliki *Protection of Children Act 1978* yang telah diperluas maknanya melalui interpretasi yurisprudensi dan revisi perundang-undangan untuk mencakup tidak hanya konten nyata, tetapi juga konten *pseudo-photographs* atau gambar yang tampak seperti anak walaupun tidak berdasarkan anak

¹⁸ Nicola Henry and Asher Flynn, "Image-Based Sexual Abuse: A Feminist Criminological Approach," *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, 1109-30, https://doi.org/10.1007/978-3-319-78440-3_47.

¹⁹ GOV.UK, *Online Safety Act Explainer*, 2024, "Duties about illegal content – the illegal content duties are now in effect ..." (diakses 7 Juni 2025).

²⁰ GOV.UK / Ofcom, *Illegal and harmful content guidance*, June 2025, "Online services must protect ... including child sexual exploitation and abuse." (diakses 7 Juni 2025).

nyata.²¹ Dengan demikian, hukum pidana Inggris tidak mensyaratkan keberadaan korban anak secara fisik untuk dapat menjatuhkan sanksi atas eksploitasi seksual.

Perbandingan antara sistem hukum Indonesia dan Inggris menunjukkan perbedaan yang cukup fundamental dalam hal pendekatan normatif terhadap AI-CSAM:

Tabel 1.

Perbandingan Hukum antara Inggris dan Indonesia Terkait Pengaturan AI-CASM

No.	Perbandingan	Inggris	Indonesia
1	Substansi	Di Inggris, konsep pseudo-photograph dan priority content telah menjangkau konten non-nyata yang tetap berbahaya secara seksual.	Di Indonesia, tidak ada ketentuan dalam UU ITE, UU Pornografi, atau UU Perlindungan Anak yang mengatur konten berbasis AI secara eksplisit.
2	Pertanggung jawaban	Inggris secara hukum positif membebankan tanggung jawab proaktif kepada penyedia layanan digital melalui kewajiban sistem pelaporan dan teknologi pendeteksi otomatis.	Indonesia belum memiliki aturan tentang kewajiban hukum platform digital dalam mendeteksi dan menanggulangi konten ilegal.
3	Lembaga Pengawas	Inggris mempercayakan Ofcom sebagai pengawas yang memiliki wewenang menjatuhkan denda dan sanksi administratif.	Ada beberapa lembaga khusus di Indonesia yang mengawasi konten digital anak, seperti Komisi Perlindungan Anak Indonesia (KPAI) dan Kementerian Komunikasi dan Digital (Komdigi) yang mengawasi peredaran konten di dunia maya.
4	Prosedur Pembuktian	Di Inggris, pendekatan berbasis audit dan teknologi telah ditanamkan dalam sistem hukum untuk menjamin akuntabilitas digital.	Di Indonesia, belum ada standar baku terkait pembuktian forensik konten AI.

Sumber: Diolah dari berbagai sumber: Government UK (2023); Ofcom (2023); Ferdinal, O. dkk. (2024); Hafiz, M. (2024); Yunita, R. (2023).

²¹ Josephin Mareta, “Mechanism of Law Enforcement in Protecting the Rights of Vulnerable Group (Child and Woman),” *Jurnal HAM* 7 (2016): 141.

Perbedaan antara Indonesia dan Inggris dalam pengaturan AI-CSAM sebagian besar disebabkan oleh perbedaan sistem hukum. Indonesia menganut sistem *civil law* yang cenderung menuntut kepastian tertulis dalam undang-undang. Sementara Inggris yang menganut *common law* lebih fleksibel dalam menyesuaikan dengan perkembangan sosial melalui yurisprudensi dan interpretasi hakim.²²

Selain itu, Inggris telah lebih dahulu mengadopsi pendekatan *multi-level regulation*, yakni integrasi antara hukum pidana, hukum administratif, dan tanggung jawab korporasi digital.²³ Indonesia masih mengandalkan hukum pidana konvensional dan belum menerapkan prinsip tanggung jawab kolektif pada platform penyedia layanan daring. Perbedaan lainnya terletak pada keberanian Inggris menggunakan pendekatan hukum berbasis risiko (*risk-based regulation*),²⁴ di mana sistem dirancang untuk mencegah pelanggaran sebelum terjadi. Sementara Indonesia masih dominan menerapkan pendekatan represif dan reaktif setelah pelanggaran terjadi.

Berbeda dengan Inggris, hukum nasional Indonesia belum mengenal klasifikasi *pseudo-content* maupun mekanisme penindakan administratif terhadap platform. Belum ada badan pengawas independen seperti Ofcom yang dapat memberikan sanksi terhadap kelalaian penyedia platform digital dalam mencegah penyebaran konten AI-CSAM. Selain itu, Indonesia juga belum menerapkan sistem pelaporan konten berbasis algoritma atau sistem penghapusan otomatis yang diatur secara hukum.

Perbedaan paling mencolok juga tampak dalam hal pembuktian. Dalam sistem hukum Inggris, konten *Deepfake* dapat dijadikan bukti digital yang sah dan telah didukung oleh prosedur standar forensik siber. Sementara itu, di Indonesia, proses pembuktian konten digital masih menghadapi berbagai tantangan teknis dan normatif, termasuk belum adanya panduan baku mengenai validitas forensik konten AI.

Menurut *Algorithmic Accountability Theory*, yang dikemukakan oleh Kate Crawford dan Ryan Calo menekankan tanggung jawab hukum terhadap entitas atau individu yang menciptakan algoritma berbahaya.²⁵ Indonesia belum mengenal konsep ini, sementara Inggris sudah memasukkannya dalam kewajiban platform. Dan kemudian menurut Teori *Digital Constitutionalism* yang dikemukakan oleh Giovanni De Gregorio memperlenakan konsep yang memperluas perlindungan hak asasi manusia di ranah digital, termasuk hak anak. Konstitusionalitas ruang digital menuntut peraturan yang sejalan dengan prinsip-prinsip HAM.²⁶

Berdasarkan hasil perbandingan dan analisis yang telah dilakukan, Indonesia perlu segera melakukan pembaruan hukum guna mengisi kekosongan hukum terkait kejahatan AI-CSAM. Pertama, perlu dilakukan revisi terhadap UU ITE, UU

²² UK Parliament, "Online Safety Act 2023," 2023.

²³ Chatham House, "Towards a Global Approach to Digital Platform Regulation," 2024.

²⁴ Herbert Smith Freehills, "Online Safety Regulation: A Global Regulatory Overview," 2025.

²⁵ Kate Crawford and Ryan Calo, "There Is a Blind Spot in AI Research," *Nature* 538, no. 7625 (October 2016): 311, <https://doi.org/10.1038/538311a>.

²⁶ Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge: Cambridge University Press, 2022), <https://doi.org/10.1017/9781009071215>.

Pornografi, dan UU Perlindungan Anak dengan memasukkan pengaturan eksplisit mengenai konten berbasis AI, termasuk definisi, bentuk perbuatan pidana, serta sanksi yang proporsional. Kedua, Indonesia perlu membentuk lembaga regulator independen yang memiliki kewenangan untuk mengawasi, menindak, dan memberi sanksi administratif terhadap platform digital yang tidak melakukan langkah-langkah preventif terhadap penyebaran AI-CSAM.

Ketiga, tanggung jawab hukum terhadap penyedia platform digital harus ditegaskan melalui ketentuan yang mengatur kewajiban implementasi sistem pelaporan, pendeteksian otomatis, serta audit konten berkala. Keempat, Indonesia perlu mengembangkan standar pembuktian forensik digital berbasis AI melalui kerja sama antara aparat penegak hukum, akademisi, dan pakar teknologi. Kelima, dalam mengadopsi prinsip-prinsip dari sistem hukum Inggris, Indonesia perlu tetap menjaga prinsip kodifikasi hukum dan asas legalitas yang menjadi karakteristik sistem *civil law*. Oleh karena itu, pembaruan hukum harus dituangkan dalam bentuk peraturan perundang-undangan yang hierarkis dan sistematis.

Pembaruan hukum terhadap AI-CSAM bukan sekadar kebutuhan teknis, melainkan sebuah keniscayaan konstitusional untuk menjaga hak-hak anak dari kekerasan berbasis teknologi. Upaya pembaruan ini juga perlu diikuti dengan penyuluhan hukum dan literasi digital kepada masyarakat, khususnya anak dan remaja sebagai kelompok rentan. Selain itu, kolaborasi internasional dalam pertukaran informasi dan harmonisasi standar regulasi global perlu diperkuat untuk menghadapi kejahatan lintas batas negara. Dengan demikian, sistem hukum Indonesia dapat berkembang menjadi lebih responsif, progresif, dan adaptif terhadap tantangan dunia digital.

Oleh karena itu, urgensi pembaruan hukum nasional Indonesia menjadi semakin nyata. Tidak hanya perluasan substansi norma hukum pidana untuk mencakup konten berbasis AI, tetapi juga penguatan infrastruktur kelembagaan, sistem pelaporan publik, perlindungan data anak, serta kerja sama lintas negara untuk deteksi lintas batas konten ilegal. Indonesia dapat mengadopsi prinsip-prinsip *dalam Online Safety Act* dan mekanisme penegakan hukum digital Inggris sebagai model reformasi hukum progresif.

Dari perbandingan ini dapat disimpulkan bahwa pendekatan hukum Inggris memberikan perlindungan hukum yang lebih komprehensif terhadap anak dalam ranah digital. Indonesia perlu belajar dari praktik tersebut agar mampu membangun sistem hukum pidana siber yang adaptif, responsif, dan mampu memberikan jaminan hukum terhadap hak-hak anak di era kecerdasan buatan.

4. Kesimpulan

Berdasarkan hasil pembahasan, dapat disimpulkan bahwa sistem hukum positif Indonesia saat ini belum secara komprehensif mengatur kejahatan berbasis kecerdasan buatan, khususnya konten kekerasan seksual terhadap anak yang dihasilkan oleh teknologi *Deepfake* atau dikenal sebagai *AI-generated child sexual abuse material* (AI-CSAM). Meskipun terdapat sejumlah ketentuan dalam UU ITE, UU Pornografi, dan UU Perlindungan Anak yang dapat digunakan sebagai dasar penindakan, norma-norma tersebut belum secara eksplisit menjangkau konten artifisial hasil manipulasi digital, sehingga menimbulkan kekosongan hukum (*rechtsvacuum*) dan ketidakpastian dalam

perlindungan hukum terhadap anak. Perbandingan dengan Inggris menunjukkan bahwa sistem hukum Indonesia tertinggal dari segi peraturan, kelembagaan, dan mekanisme penegakan. Inggris telah menetapkan aturan khusus yang mengatur kewajiban platform digital, menetapkan standar konten ilegal berbasis AI, serta membentuk lembaga independen untuk pengawasan. Sementara itu, Indonesia belum memiliki mekanisme serupa yang dapat menanggulangi kejahatan serupa secara preventif dan sistematis. Dengan mempertimbangkan kondisi tersebut, Indonesia perlu segera melakukan pembaruan hukum melalui revisi undang-undang terkait, pembentukan lembaga pengawasan independen, serta penguatan mekanisme pelaporan, pembuktian, dan penindakan terhadap pelaku. Langkah ini penting untuk memastikan bahwa anak-anak terlindungi secara maksimal dari eksploitasi seksual digital, serta menjamin hadirnya sistem hukum nasional yang adaptif dan relevan terhadap tantangan teknologi masa kini.

References

- Alexander Diel et al., "Human Performance in Detecting Deepfakes: A Systematic Review and Meta-Analysis of 56 Papers," *Computers in Human Behavior Reports* 16 (2024): 100538. <https://doi.org/10.1016/j.chbr.2024.100538>
- Cahyono, Soetardi Tri, Wina Erni, and Taufik Hidayat. "RIKONSTRUKSI HUKUM PIDANA TERHADAP KEJAHATAN SIBER (CYBER CRIME) DALAM SISTEM PERADILAN PIDANA INDONESIA: Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia." *Dame Journal of Law* 1, no. 1 (2025): 1–23.
- Chairani, Meirza Aulia, Krista Yitawati, and Angga Pramodya Pradhana. "Urgensi Pengaturan Hukum Bagi Penyalahgunaan Aplikasi Deepfake." *Jurnal Rechts* 13, no. 1 (2024). <https://doi.org/10.56013/rechts.v13i1.2668>.
- Chatham House. "Towards a Global Approach to Digital Platform Regulation," 2024.
- Crawford, Kate, and Ryan Calo. "There Is a Blind Spot in AI Research." *Nature* 538, no. 7625 (October 2016): 311. <https://doi.org/10.1038/538311a>.
- Dewi Tresnawati et al., "Artificial Intelligence Serta Singularitas Suatu Kekeliruan Atau Tantangan," *Jurnal Algoritma* 19, no. 1 (2022): 181–88. <https://doi.org/10.33364/algoritma/v.19-1.1028>
- Diel, Alexander, Tania Lalg, Isabel Carolin Schröter, Karl F MacDorman, Martin Teufel, and Alexander Bäuherle. "Human Performance in Detecting Deepfakes: A Systematic Review and Meta-Analysis of 56 Papers." *Computers in Human Behavior Reports* 16 (2024): 100538.
- Fauzyah, Rizgita Nurul, Putri Hafidati, and Sunarya Sunarya. "Perlindungan Hukum Terhadap Korban Tindak Pidana Pembuat Video Pornografi Palsu (Deepfake Porn) Berbasis Artificial Intelligence (AI) Di Indonesia." *Lex Veritatis* 3, no. 3 (2024): 74–88.
- Fitri, Dwi, Syakban Akbar, Nawal Mufidah, Rezita Ardhani Manurung, Dara Akila, Sania Izzati Ramadhani, Nazwa Hanifah Tanjung, Aulia Putri, Ade Nur Hidayah, and Muhammad Zikri. "Deepfake Dan Krisis Kepercayaan: Analisis Hukum Terhadap Penyebaran Konten Palsu Di Media Sosial." *Jurnal Intelek Insan Cendikia* 2, no. 6 (2025): 11556–68.
- Foundation, Internet Watch. "IWF Annual Report 2022," 2022. <https://www.iwf.org.uk/about-us/who-we-are/annual-report-2022/>.

- Gregorio, Giovanni De. *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*. Cambridge: Cambridge University Press, 2022. <https://doi.org/10.1017/9781009071215>.
- Hailtik, Asri Gresmelian Eurike, and Wiwik Afifah. "Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia." *Asian Journal of Social and Humanities* 2, no. 4 (2023): 776–95.
- Henry, Nicola, and Asher Flynn. "Image-Based Sexual Abuse: A Feminist Criminological Approach." *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, 1109–30. https://doi.org/10.1007/978-3-319-78440-3_47.
- Herbert Smith Freehills. "Online Safety Regulation: A Global Regulatory Overview," 2025.
- Isnawan, Fuadi. "Deepfake Pornography: How Criminal Liability of Perpetrators in the Indonesian Criminal Law Framework." *Jurnal Magister Hukum Udayana*, 2024. <https://doi.org/10.24843/JMHU.2024.v13.i03.p15>.
- Judijanto, Loso, and Rabith Madah Khulaili Harsya. "Etika Dan Hukum Dalam Penggunaan Artificial Intelligence Terhadap Privasi Digital Di Indonesia." *Sanskara Hukum Dan HAM* 3, no. 03 (2025): 141–49.
- Lase, Satria Muhammad Nur, Aisyah Adinda, and Rizkia Diffa Yuliantika. "Kerangka Hukum Teknologi Blockchain Berdasarkan Hukum Siber Di Indonesia." *Padjadjaran Law Review* 9, no. 1 (2021).
- Mareta, Josephin. "Mechanism of Law Enforcement in Protecting the Rights of Vulnerable Group (Child and Woman)." *Jurnal HAM* 7 (2016): 141.
- Panjaitan, Kevin Amos Alexander, Prija Djatmika, and Alfons Zakaria. "Urgensi Pengaturan Hukum Terhadap Korban Tindak Pidana Pornografi Deepfake Di Indonesia." *Universitas Brawijaya*, 2025.
- Peter Mahmud Marzuki. *Penelitian Hukum Edisi Revisi*. Jakarta: Kencana, 2017.
- Putra, Izil Hidayat. "Perlindungan Hukum Terhadap Korban Penyalahgunaan Artificial Intelligence (AI) Berupa Deepfake Pornografi Menurut Peraturan Perundang-Undangan." *UNJA Journal of Legal Studies* 1, no. 2 (2024): 110–28.
- Syahirah, Sabrina Nur, and Bayu Prasetyo. "TINJAUAN YURIDIS TERHADAP PENGGUNAAN TEKNOLOGI DEEPPAKE UNTUK PORNOGRAFI MELALUI ARTIFICIAL INTELLIGENCE (AI) DI INDONESIA." *Jurnal Inovasi Hukum Dan Kebijakan* 6, no. 1 (2025).
- Tresnawati, Dewi, Yomi Guno, I Putu Satwika, Ary Setijadi Prihatmanto, and Dimitri Mahayana. "Artificial Intelligence Serta Singularitas Suatu Kekeliruan Atau Tantangan." *Jurnal Algoritma* 19, no. 1 (2022): 181–88.
- Trivison, Amy. "Understanding the Line Between Art and Abuse: How Generative AI Changes the Landscape of Child Sexual Abuse Materials." *Catholic University Journal of Law and Technology* 33, no. 1 (2024): 87–114.
- UK Parliament. "Online Safety Act 2023," 2023.
- Vanna, Francesco De. "The Construction of a Normative Framework for Technology-Driven Innovations: A Legal Theory Perspective." *Use and Misuse of New Technologies: Contemporary Challenges in International and European Law*, 2019, 185–208.
- Wahyudi, B R. "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI." *Innovative: Journal Of Social Science Research* 5, no. 1 (2025): 3436–50.
- Wibowo, Agus, and Sri Yulianingsih. "Hukum Teknologi Informasi." *Penerbit Yayasan Prima Agus Teknik*, 2025.

Peraturan Perundang-undangan

- Kitab Undang-Undang Hukum Pidana (KUHP). Wetboek van Strafrecht (Staatsblad Tahun 1915 Nomor 732) Undang-Undang Nomor 1 Tahun 1946 tentang Kitab Undang-Undang Hukum Pidana sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1.
- Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Tambahan Lembaran Negara Republik Indonesia Nomor 4843.
- Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251. Tambahan Lembaran Negara Republik Indonesia Nomor 5952.
- Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 3. Tambahan Lembaran Negara Republik Indonesia Nomor 6883.
- Undang-Undang Republik Indonesia Nomor 35 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak. Lembaran Negara Republik Indonesia Tahun 2014 Nomor 297. Tambahan Lembaran Negara Republik Indonesia Nomor 5606.
- Undang-Undang Republik Indonesia Nomor 17 Tahun 2016 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2016 tentang Perubahan Kedua atas Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak menjadi Undang-Undang. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 237. Tambahan Lembaran Negara Republik Indonesia Nomor 5946.
- Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang Pornografi. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 181. Tambahan Lembaran Negara Republik Indonesia Nomor 4928.
- United Kingdom. Online Safety Act 2023. Chapter 50. London: The Stationery Office.
- United Kingdom. Protection of Children Act 1978. Chapter 37. London: The Stationery Office.