DOI: https://doi.org/10.62017/merdeka

Tindak Pidana Deepfake Pornography di Indonesia: Analisis Yuridis terhadap Kekosongan Norma dalam KUHP dan UU ITE

Muhammad Afif *[1]

[1] Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pembangunan "Veteran" Jakarta
*e-mail : 2310611138@mahasiswa.upnvj.ac.id

Abstrak

Kemajuan teknologi kecerdasan buatan (Artificial Intelligence/AI) telah melahirkan fenomena deepfake pornography, yaitu manipulasi audio-visual yang menampilkan seseorang dalam konten pornografi tanpa persetujuannya. Di Indonesia, meskipun regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pornografi, dan Kitab Undang-Undang Hukum Pidana (KUHP) telah mengatur pornografi dan konten elektronik, belum terdapat norma yang secara eksplisit mengatur dan mengkualifikasi deepfake pornography. Penelitian ini bertujuan melakukan analisis yuridis terhadap kekosongan norma (legal vacuum) dalam KUHP dan UU ITE serta implikasinya terhadap penegakan hukum. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan statute approach dan studi literatur. Hasil penelitian menunjukkan bahwa ketentuan yang ada tidak memadai karena tidak mencakup manipulasi berbasis AI sebagai elemen delik, sehingga pelaku sulit dipidana dan korban sulit mendapatkan perlindungan hukum yang memadai. Untuk itu perlu dilakukan reformasi regulasi, termasuk memasukkan delik khusus dan memperkuat mekanisme forensik digital.

Kata Kunci : *deepfake pornography, kekosongan norma, KUHP, UU ITE, hukum pidana Indonesia*

Abstract

The advancement of Artificial Intelligence (AI) technology has given rise to the phenomenon of deepfake pornography, which involves audio-visual manipulation depicting a person in pornographic content without their consent. In Indonesia, although regulations such as the Information and Electronic Transactions Law (ITE Law), the Pornography Law, and the Criminal Code (KUHP) regulate pornography and electronic content, there is no specific norm that explicitly addresses and qualifies deepfake pornography. This study aims to conduct a juridical analysis of the normative gap (legal vacuum) in the KUHP and the ITE Law and its implications for law enforcement. The method used is normative legal research with a statute-approach and literature study. The findings indicate that existing provisions are inadequate because they do not cover AI-based manipulation as a constituent of the offense, making it difficult to prosecute perpetrators and protect victims. Therefore, regulatory reform is needed, including introducing a specific offense and strengthening digital forensic mechanisms.

Keywords*: deepfake pornography, normative gap, KUHP, ITE Law, Indonesian criminal law*

PENDAHULUAN

Fenomena *deepfake* muncul sebagai salah satu hasil dari perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*/AI) yang mampu memanipulasi data visual dan audio dengan tingkat realisme yang sangat tinggi. Teknologi ini memungkinkan penggantian wajah seseorang dalam gambar atau video secara digital hingga tampak seolah-olah asli. Dalam konteks tertentu, kemampuan ini memang dapat dimanfaatkan untuk tujuan positif seperti industri film, pendidikan, dan hiburan. Namun, ketika disalahgunakan, teknologi ini menjadi ancaman serius bagi hak privasi dan kehormatan individu, terutama melalui munculnya fenomena *deepfake pornography* yakni pembuatan dan penyebaran konten pornografi palsu yang menampilkan wajah seseorang tanpa persetujuan mereka.[1]

Laporan *The State of Deepfakes* yang diterbitkan oleh Deeptrace pada tahun 2019 menunjukkan bahwa 96% dari seluruh video deepfake yang beredar di internet mengandung unsur pornografi, dan sebagian besar menargetkan perempuan sebagai korban.[2] Angka ini

[1] Chesney, R., & Citron, D. K. (2019). *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security.* California Law Review, 107(6), 1753–1820.
[2] Deeptrace. (2019). *The State of Deepfakes: Landscape, Threats, and Impact.* Amsterdam: Deeptrace Labs.

DOI: https://doi.org/10.62017/merdeka

mengindikasikan bahwa teknologi AI tidak hanya berkembang secara cepat, tetapi juga telah digunakan untuk melakukan bentuk kekerasan berbasis gender dalam ranah digital. Korban deepfake pornography umumnya mengalami dampak sosial dan psikologis berat, seperti trauma, kehilangan pekerjaan, atau bahkan pengucilan sosial.

Di Indonesia, kasus serupa mulai bermunculan di berbagai platform media sosial. Akan tetapi, sebagian besar kasus tersebut tidak dapat diproses secara hukum karena tidak ada pasal dalam KUHP maupun UU ITE yang secara eksplisit mengatur tentang pembuatan dan penyebaran konten palsu berbasis AI. Misalnya, Pasal 27 ayat (1) UU ITE hanya mengatur larangan penyebaran konten yang melanggar kesusilaan, tanpa menyebutkan secara spesifik bentuk konten yang dimanipulasi secara digital.[3] Dalam praktiknya, pelaku dapat beralasan bahwa video yang dibuat hanyalah bentuk "rekayasa" atau "hiburan", bukan konten pornografi sungguhan, sehingga sulit untuk dijerat hukum.

Kondisi ini menimbulkan kekosongan norma hukum (legal vacuum), yaitu situasi ketika suatu perbuatan yang jelas menimbulkan kerugian sosial tidak memiliki dasar hukum yang memadai untuk dilakukan penindakan. Kekosongan norma semacam ini memperlihatkan lemahnya kemampuan sistem hukum pidana Indonesia dalam beradaptasi dengan perkembangan teknologi digital yang sangat cepat.[4]

Selain persoalan normatif, tantangan lain juga muncul dari aspek pembuktian. Pembuktian dalam kasus *deepfake pornography* menuntut kemampuan forensik digital yang mumpuni untuk membuktikan keaslian konten serta niat pelaku (*mens rea*). Dalam praktik penegakan hukum di Indonesia, kemampuan ini masih terbatas, baik dari sisi peralatan maupun keahlian sumber daya manusia.[5] Hal ini membuat korban semakin sulit memperoleh keadilan, karena pelaku dapat bersembunyi di balik kompleksitas teknologi yang digunakan.

Berdasarkan latar belakang tersebut, tulisan ini berupaya menganalisis secara yuridis kekosongan norma dalam KUHP dan UU ITE terhadap tindak pidana deepfake pornography, serta menelaah urgensi pembaharuan hukum pidana nasional agar lebih responsif terhadap perkembangan kejahatan berbasis AI. Adapun tujuan dari penelitian ini untuk menganalisis dasar pengaturan hukum pidana yang berlaku di Indonesia terhadap fenomena deepfake pornography, mengidentifikasi bentuk kekosongan norma hukum yang menyebabkan lemahnya penegakan hukum dan menawarkan kerangka konseptual pembaruan hukum pidana berbasis teknologi kecerdasan buatan.

Sedangkan ruang lingkup tulisan dibatasi pada kajian hukum pidana nasional dengan fokus terhadap dua regulasi utama, yaitu Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), serta relevansinya terhadap fenomena kejahatan digital dalam bentuk *deepfake pornography*.

METODE

Penelitian ini menggunakan pendekatan yuridis normatif, karena fokus utamanya adalah menelaah dan menganalisis peraturan perundang-undangan yang berlaku, serta kesesuaian norma hukum tersebut dengan fenomena sosial yang berkembang akibat kemajuan teknologi digital. Pendekatan ini dipilih karena permasalahan yang dikaji, yakni tindak pidana *deepfake pornography* berkaitan langsung dengan kekosongan hukum dalam sistem perundang-undangan nasional, bukan pada peristiwa empiris atau data lapangan. Dengan kata lain, penelitian ini berusaha menjawab pertanyaan, sejauh mana hukum positif Indonesia saat ini mampu menjangkau bentuk kejahatan baru yang lahir dari perkembangan kecerdasan buatan.

Dalam penelitian hukum normatif, sumber utama yang digunakan adalah bahan hukum primer berupa peraturan perundang-undangan seperti Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[3] Mahendra, A. (2023). *Analisis Yuridis terhadap Kejahatan Siber dan Kekosongan Norma dalam UU ITE.* Jurnal Hukum Teknologi, 8(2), 112–128.
[4] Muladi. (2021). *Hukum Pidana dan Perkembangan Teknologi Informasi.* Bandung: Alumni.
[5] Setiadi, H. (2024). *Forensik Digital dalam Pembuktian Tindak Pidana Siber.* Jurnal Ilmu Hukum dan Teknologi, 6(1), 75–89.

beserta perubahannya, serta Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi. Ketiga regulasi tersebut merupakan instrumen utama dalam sistem hukum pidana Indonesia yang secara teoritis dapat digunakan untuk menjerat pelaku kejahatan kesusilaan, termasuk penyebaran konten bermuatan pornografi. Namun, penelitian ini berangkat dari dugaan bahwa norma-norma tersebut belum sepenuhnya mampu menampung kejahatan digital seperti *deepfake pornography* yang bersifat manipulatif dan tidak nyata.

Selain itu, digunakan juga bahan hukum sekunder seperti buku-buku hukum pidana, artikel ilmiah, jurnal hukum, laporan riset dari lembaga siber nasional, serta tulisan akademik yang membahas kejahatan digital dan perkembangan hukum siber. Bahan hukum sekunder ini digunakan untuk memperkuat analisis teoritis dan memberikan gambaran komparatif antara Indonesia dan negara lain yang telah memiliki regulasi mengenai *deepfake* atau kejahatan siber berbasis kecerdasan buatan. Misalnya, Korea Selatan dan Inggris telah mengatur secara tegas larangan distribusi konten hasil rekayasa digital yang melanggar privasi seseorang. Dari sana, penulis membandingkan sejauh mana pendekatan hukum Indonesia masih tertinggal dibanding praktik hukum internasional.[6]

Untuk memperkaya sudut pandang, penelitian ini juga menggunakan pendekatan konseptual (*conceptual approach*), yakni mengkaji konsep-konsep dasar yang melandasi perumusan delik kesusilaan dan perlindungan privasi. Pendekatan ini diperlukan karena munculnya *deepfake pornography* tidak sekadar menimbulkan persoalan teknis hukum, tetapi juga persoalan moral dan hak asasi manusia. Deepfake bukan hanya pelanggaran terhadap kesusilaan publik, melainkan juga serangan terhadap martabat individu dan hak atas privasi yang dijamin dalam Pasal 28G ayat (1) UUD 1945. Karena itu, penelitian ini menempatkan *deepfake pornography* sebagai isu hukum yang bersifat multidimensional, mencakup aspek hukum pidana, hak asasi manusia, dan etika digital.[7]

Melalui metode ini, penelitian diharapkan mampu memberikan pemahaman yang lebih mendalam mengenai posisi hukum Indonesia dalam menghadapi kejahatan digital, sekaligus menjadi dasar argumentatif bagi urgensi pembentukan norma baru terkait *deepfake pornography*. Pendekatan yuridis normatif yang dilengkapi dengan analisis konseptual dan perbandingan internasional diharapkan dapat menghadirkan solusi hukum yang tidak hanya sesuai dengan asas legalitas, tetapi juga sejalan dengan prinsip keadilan dan perlindungan hak asasi manusia di era teknologi informasi yang semakin kompleks.

HASIL DAN PEMBAHASAN

1. Pengaturan Hukum Pidana di Indonesia terhadap Penyebaran Konten Deepfake Pornography

Fenomena *deepfake pornography* merupakan salah satu bentuk kejahatan siber yang paling kompleks di era kecerdasan buatan (Artificial Intelligence/AI). Istilah *deepfake* berasal dari gabungan kata "deep learning" dan "fake," yang berarti hasil manipulasi visual berbasis algoritma *machine learning* yang mampu meniru wajah seseorang dan menempelkan pada tubuh orang lain secara sangat realistis. Dalam konteks pornografi, teknologi ini digunakan untuk menciptakan konten seksual palsu dengan menampilkan wajah korban seolah-olah sedang melakukan tindakan asusila. Dampak yang ditimbulkan tidak hanya berupa kerugian moral dan psikologis, tetapi juga kerusakan reputasi yang sulit dipulihkan, terutama karena penyebarannya di ruang digital bersifat viral dan sulit dihapus sepenuhnya.[8]

Sayangnya, pengaturan hukum pidana di Indonesia belum sepenuhnya siap menghadapi modus kejahatan digital semacam ini. Hingga saat ini, belum terdapat norma hukum positif yang secara eksplisit mengatur tentang *deepfake pornography*. Regulasi yang paling sering digunakan

[6] Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). *Deepfakes: Trick or treat? Business Horizons*, 63(2), 135–146. https://doi.org/10.1016/j.bushor.2019.11.006

[7] Setiadi, W. (2023). *Tantangan Hukum Siber di Indonesia dalam Menghadapi Kejahatan Deepfake. Jurnal Hukum & Teknologi*, 8(1), 44–59

[8] Chesney, R., & Citron, D. K. (2019). *Deep Fakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics.* Foreign Affairs, 98(1), 147–155.

DOI: https://doi.org/10.62017/merdeka

adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah dengan UU Nomor 19 Tahun 2016, terutama Pasal 27 ayat (1) yang menyebutkan bahwa *"Setiap orang dilarang mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan melanggar kesusilaan."*

Namun, pasal ini sejatinya masih menimbulkan multitafsir karena tidak secara tegas mengakomodasi keberadaan konten hasil rekayasa digital berbasis AI. Dalam praktiknya, pasal ini lebih sering diterapkan pada kasus penyebaran video porno asli atau konten asusila konvensional. Sementara dalam kasus *deepfake*, unsur kesusilaan yang dimaksud menjadi kabur karena objeknya adalah konten palsu yang tidak melibatkan tindakan nyata. Aparat penegak hukum pun sering kali kesulitan membuktikan unsur kesengajaan dan keterlibatan pelaku utama, mengingat proses pembuatan *deepfake* bisa dilakukan secara anonim melalui platform luar negeri atau perangkat lunak open-source.

Dari sisi KUHP, ketentuan mengenai kesusilaan termuat dalam Pasal 281–282 KUHP, namun substansi pasal-pasal tersebut hanya mengatur perilaku cabul di tempat umum atau penyebaran benda yang "melanggar kesusilaan" dalam bentuk fisik. Artinya, pasal-pasal tersebut disusun dalam konteks kejahatan konvensional, bukan untuk menjawab tantangan kejahatan digital. Ketika objek kejahatan berubah menjadi hasil algoritma komputer, hukum positif menjadi tumpul karena unsur-unsurnya tidak terpenuhi secara tekstual. Akibatnya, *deepfake pornography* sering tidak dianggap sebagai tindak pidana murni, melainkan hanya pelanggaran terhadap kesusilaan umum di ruang digital.

Dalam kasus tertentu, aparat penegak hukum bahkan hanya bisa menjerat pelaku dengan pasal pencemaran nama baik atau penyebaran berita bohong sebagaimana diatur dalam Pasal 27 ayat (3) dan (4) UU ITE, padahal motif dan akibat dari *deepfake pornography* sangat berbeda. Hal ini menimbulkan problem yuridis dan moral, karena korban yang wajahnya direkayasa menjadi seolah pelaku pornografi justru tidak mendapatkan perlindungan hukum yang proporsional. Sebagai contoh nyata, pada tahun 2023 beredar video *deepfake* yang menampilkan beberapa figur publik perempuan Indonesia. Kasus ini ramai di media sosial dan menimbulkan trauma bagi para korban, namun kepolisian mengakui kesulitan untuk memproses secara hukum karena belum ada norma pidana yang mengatur *deepfake* secara eksplisit. Situasi ini memperlihatkan bahwa hukum pidana Indonesia masih tertinggal dibandingkan dengan dinamika kejahatan digital yang semakin canggih dan lintas batas.

2. Perbandingan Penanganan Deepfake

Dalam menilai kemampuan sebuah sistem hukum menangani *deepfake pornography*, ada beberapa variabel penting yang perlu diperhatikan: kepastian normatif (apakah ada undang-undang yang eksplisit mengatur deepfake), mekanisme penegakan (apakah aparat memiliki alat dan kapasitas forensik untuk membuktikan kejahatan ini), peran platform digital (kewajiban penyedia layanan untuk menghapus/menandai konten), dan akses pemulihan bagi korban (mekanisme penghapusan, kompensasi, atau pemulihan reputasi). Bila variabel-variabel ini dikomparasikan antara Indonesia dan sejumlah negara yang sudah lebih dulu bereaksi terhadap fenomena deepfake, terlihat perbedaan tajam yang menjelaskan mengapa beberapa yurisdiksi lebih efektif dalam memberikan perlindungan cepat kepada korban.

Di Indonesia, landasan hukum yang selama ini dipakai untuk menjerat penyebar *deepfake pornography* bersandar pada ketentuan umum tentang kesusilaan dalam KUHP dan pada Pasal 27 UU ITE yang melarang pendistribusian konten yang "melanggar kesusilaan". Namun, teks undang-undang belum pernah secara eksplisit merumuskan pembuatan atau distribusi konten sintetis (AI-generated) sebagai delik tersendiri sehingga aparat sering bergulat dengan masalah interpretasi unsur delik; apakah konten yang "hanya" direkayasa dapat dikualifikasikan sebagai pornografi, pencemaran nama baik, atau penipuan, dan bagaimana membuktikan unsur kesengajaan pembuatnya. Hal praktisnya adalah kasus-kasus yang menjadi viral kerap berujung pada kesulitan penyidikan karena pelaku bekerja lintas batas dan dengan alat yang mudah diperoleh, sementara kemampuan forensik digital untuk menganalisis bukti masih terbatas di

DOI: https://doi.org/10.62017/merdeka

banyak lembaga penegak hukum nasional. Selain itu, kewajiban platform digital untuk secara proaktif menghapus atau menandai konten deepfake belum diatur secara tegas, sehingga proses penghapusan sering bergantung pada mekanisme internal platform atau permintaan hukum yang lambat.

Bandingkan situasi itu dengan beberapa yurisdiksi lain. Di Amerika Serikat respons terhadap deepfake lebih terfragmentasi karena tidak ada undang-undang federal tunggal yang mengatur semua bentuk deepfake, pemecahan masalah dilakukan di tingkat negara bagian (state). Sejak Virginia menjadi pionir pada 2019, sebagian besar negara bagian AS telah mengesahkan aturan yang melarang pembuatan dan/atau penyebaran *non-consensual deepfake pornography* dan/atau menempatkan kewajiban sivil bagi penyebar. Hingga 2025, puluhan negara bagian telah memiliki ketentuan semacam itu: beberapa fokus pada perlindungan terhadap korban dewasa, beberapa memasukkan anak di bawah umur, dan beberapa memadukan sanksi pidana dengan jalur perdata untuk kompensasi korban. Selain itu, sebagian yurisdiksi AS memadukan langkah hukum dengan mekanisme cepat (mis. perintah pengadilan darurat untuk penghapusan konten). Kekuatan lain di AS adalah ketersediaan litigasi perdata (tuntutan ganti rugi) yang memberi jalur remedial selain pidana, walau kebebasan berbicara (First Amendment) tetap menjadi batas yang harus dihadapi pembuat undang-undang.

Inggris Raya menempuh jalur penegakan yang relatif keras dalam praktik—kasus-kasus yang melibatkan pembuatan materi seksual anak hasil AI misalnya telah menghasilkan hukuman berat dan preseden pidana penting, menunjukkan bahwa sistem peradilan Inggris siap memanfaatkan pasal terkait kejahatan seksual bahkan bila materi itu sebagian dihasilkan oleh komputer. Vonis-vonis ini memberi sinyal kuat bahwa pembuatan dan distribusi materi intim palsu, apalagi yang berkaitan dengan eksploitasi anak, akan ditangani dengan serius oleh aparat penegak hukum Inggris.

Korea Selatan mengambil pendekatan hukum yang lebih agresif dalam beberapa tahun terakhir: selain menjerat pembuat dan distributor, Korea Selatan juga mengkriminalisasi kepemilikan atau penonton materi deepfake tertentu, sebagai respons terhadap fenomena grup-grup di aplikasi pesan yang menyebarkan deepfake massal. Legislasi semacam ini menunjukkan paradigma perlindungan publik yang lebih luas—bukan sekadar menghukum pembuat, tetapi juga membatasi permintaan dan sirkulasi konten berbahaya dalam masyarakat.

Australia menggerakkan revisi legislasi perlindungan online dan membahas ancaman serius dari distribusi deepfake pornographic. Pemerintah mengusulkan atau menerapkan undang-undang yang secara khusus memidana pembuatan dan penyebaran deepfake pornografi tanpa persetujuan, dengan ancaman hukum yang relatif berat serta mekanisme penghapusan cepat melalui badan pengawas keselamatan online (eSafety Commissioner) yang memiliki kewenangan relatif kuat untuk memerintahkan penghapusan konten.

Di tingkat supranasional, Uni Eropa menaruh perhatian pada risiko-risiko yang ditimbulkan oleh konten sintetis. Meskipun AI Act (dan aturan keselamatan daring lain) tidak secara eksplisit mengkriminalisasi semua deepfake pornography, kerangka peraturan tersebut mengatur kewajiban transparansi dan mitigasi risiko pada penyedia layanan AI dan platform, serta memberi ruang hukum bagi tindakan proaktif, misalnya kewajiban menandai konten sintetis atau melaksanakan proses notice-and-takedown yang lebih cepat untuk konten berbahaya.

Dari perbandingan itu, beberapa pelajaran praktis muncul bagi Indonesia. Pertama, yurisdiksi yang lebih berhasil menangani masalah deepfake biasanya memiliki definisi hukum yang jelas, mencakup pembuatan, distribusi, dan kepemilikan materi sintetis tanpa persetujuan sebagai delik yang dapat dikenai sanksi pidana dan/atau perdata. Kedua, keberadaan mekanisme remedial cepat, perintah pengadilan darurat, kewenangan lembaga pengawas untuk memerintahkan penghapusan, atau jalur perdata yang memudahkan kompensasi, membantu mengurangi kerusakan reputasi korban yang terjadi seketika begitu konten viral. Ketiga, negara-negara yang efektif menggabungkan penegakan hukum dengan peningkatan kapasitas forensik digital dan kerja sama internasional sehingga dapat melacak asal konten lintas batas. Keempat, regulasi yang menempatkan tanggung jawab pada platform misalnya melalui kewajiban deteksi

otomatis atau sistem pelaporan yang efisien, mempercepat mitigasi penyebaran konten, walau menimbulkan tantangan terhadap kebebasan berekspresi dan isu teknis seperti false positives.

3. Kekosongan Norma Hukum dalam KUHP dan UU ITE terhadap Fenomena Deepfake Pornography

Kekosongan norma hukum (*legal vacuum*) terhadap fenomena *deepfake pornography* merupakan konsekuensi logis dari lambatnya adaptasi sistem hukum terhadap perkembangan teknologi digital. Meskipun KUHP dan UU ITE sama-sama mengatur larangan atas konten yang melanggar kesusilaan, keduanya tidak memberikan landasan normatif yang memadai untuk menjerat pelaku yang memproduksi dan menyebarkan konten seksual palsu menggunakan wajah orang lain tanpa izin.

Dalam KUHP, konsep "melanggar kesusilaan" yang diatur dalam Pasal 282 masih berpijak pada paradigma moralitas publik konvensional. Hukum ini hanya mengenal bentuk pelanggaran yang nyata dan konkret, seperti memperlihatkan perbuatan cabul atau mendistribusikan gambar porno secara langsung. Sedangkan *deepfake pornography* bekerja di ranah representasi digital, wajah seseorang ditempelkan secara realistis ke tubuh lain, sehingga tidak ada tindakan cabul yang benar-benar dilakukan oleh korban. Dengan demikian, unsur "perbuatan cabul" atau "kesusilaan" dalam KUHP sulit diterapkan secara analogis tanpa melanggar asas legalitas dalam hukum pidana.[9]

Sementara itu, dalam UU ITE, meskipun Pasal 27 ayat (1) tampak relevan, undang-undang ini tidak mengenal konsep "rekayasa digital" sebagai objek hukum. UU ITE lebih fokus pada aspek distribusi informasi, bukan pada keaslian atau keabsahan konten. Hal ini menyebabkan aparat hukum tidak memiliki dasar hukum yang cukup untuk menghukum pembuat *deepfake* apabila konten tersebut belum disebarkan secara luas. Artinya, pembuat video bisa bebas dari jerat hukum meskipun telah melakukan pelanggaran terhadap privasi seseorang.

Masalah ini semakin kompleks karena tidak ada pengaturan yang eksplisit tentang hak atas citra (*right of likeness*) dalam hukum Indonesia. Hak privasi dan citra seseorang memang telah dijamin secara konstitusional melalui Pasal 28G ayat (1) UUD 1945, namun jaminan tersebut belum diterjemahkan secara konkret dalam hukum pidana. Berbeda dengan sistem hukum di negara lain seperti Amerika Serikat atau Korea Selatan yang telah memiliki undang-undang khusus untuk menindak *non-consensual deepfake pornography*, Indonesia masih mengandalkan tafsir terhadap norma-norma umum.[10]

Ketiadaan norma ini bukan hanya menyebabkan pelaku sulit dijerat, tetapi juga menimbulkan *reviktimisasi* terhadap korban. Banyak korban justru dipersalahkan atau diragukan kredibilitasnya karena konten yang beredar tampak nyata, padahal sepenuhnya hasil manipulasi digital. Dalam beberapa kasus, korban bahkan menghadapi ancaman sosial dan kehilangan pekerjaan akibat reputasi yang rusak. Hukum yang seharusnya menjadi pelindung justru tidak memiliki instrumen yang efektif untuk memberikan keadilan. Kekosongan norma hukum tersebut menegaskan pentingnya pembaruan regulasi yang mampu mengantisipasi perkembangan teknologi. Jika tidak, hukum pidana akan terus tertinggal dan kehilangan fungsinya sebagai alat kontrol sosial yang adil.

4. Arah Pembaruan Hukum Pidana yang Ideal untuk Mengantisipasi Kejahatan Digital Berbasis AI

Perkembangan teknologi kecerdasan buatan (Artificial Intelligence/AI) membawa perubahan besar dalam berbagai aspek kehidupan manusia. Namun, di balik kemajuan tersebut, muncul pula tantangan baru yang mengancam keamanan, privasi, dan martabat manusia, salah satunya dalam bentuk *deepfake pornography*. Fenomena ini merupakan hasil manipulasi teknologi yang mampu menciptakan rekayasa visual atau audio sedemikian rupa sehingga

[9] Simanjuntak, P. (2022). *Kejahatan Digital dan Kekosongan Norma Hukum Pidana Indonesia.* Jurnal Ilmu Hukum Lex Renaissance, 7(2), 201–218.
[10] Setiadi, W. (2023). *Tantangan Hukum Siber di Indonesia dalam Menghadapi Kejahatan Deepfake.* Jurnal Hukum & Teknologi, 8(1), 44–59.

DOI: https://doi.org/10.62017/merdeka

tampak nyata, padahal sepenuhnya palsu. Ketika wajah atau tubuh seseorang dimanipulasi untuk dimasukkan ke dalam konten pornografi tanpa izin, yang terjadi bukan hanya pelanggaran terhadap kesusilaan, tetapi juga serangan terhadap identitas, privasi, serta integritas pribadi korban. Karena itu, arah pembaruan hukum pidana di Indonesia perlu diarahkan untuk menjawab kompleksitas kejahatan digital yang berbasis AI dengan pendekatan yang lebih adaptif, holistik, dan berorientasi pada perlindungan manusia.

Selama ini, sistem hukum pidana cenderung bersifat reaktif, yaitu baru bertindak ketika kejahatan telah terjadi. Namun, karakteristik teknologi AI yang bergerak cepat dan sulit dikendalikan menuntut sistem hukum yang lebih antisipatif. *Deepfake pornography* menjadi contoh nyata bagaimana hukum yang statis tidak mampu mengikuti dinamika teknologi yang sangat cair. Saat pelaku dapat membuat dan menyebarkan konten palsu hanya dengan perangkat sederhana dan waktu yang singkat, korban kerap kali kehilangan kendali atas citra dirinya di dunia maya. Dalam konteks inilah, hukum pidana Indonesia perlu menyesuaikan diri, tidak hanya dengan memperbarui pasal-pasal yang ada, tetapi juga dengan merumuskan pendekatan baru yang memahami karakteristik teknologi digital.

Langkah pertama yang perlu dilakukan negara adalah merumuskan regulasi khusus yang secara tegas mengatur kejahatan berbasis kecerdasan buatan. Regulasi ini harus memiliki definisi yang jelas mengenai *deepfake*, unsur-unsur perbuatan yang dapat dikategorikan sebagai tindak pidana, serta bentuk tanggung jawab pidana bagi berbagai pihak yang terlibat, baik pembuat, penyebar, maupun pihak yang memperoleh keuntungan dari penyebaran konten tersebut. Ketegasan hukum ini penting agar tidak terjadi kekosongan norma yang dapat dimanfaatkan pelaku untuk menghindari pertanggungjawaban. Lebih jauh, regulasi semacam ini juga perlu mengatur kewajiban bagi platform digital untuk secara proaktif mendeteksi, menandai, dan menghapus konten *deepfake pornography* yang beredar di ruang siber mereka.[11] Artinya, tanggung jawab hukum tidak hanya dibebankan kepada individu, tetapi juga kepada korporasi digital yang menjadi perantara peredaran informasi.

Selain pengaturan hukum yang bersifat represif, pembaruan hukum juga harus mengedepankan nilai-nilai kemanusiaan, terutama dalam hal perlindungan hak privasi dan martabat manusia. Kejahatan digital seperti *deepfake pornography* bukan sekadar persoalan kesusilaan, tetapi juga bentuk kekerasan berbasis gender dan pelanggaran hak asasi manusia. Korban tidak hanya mengalami kerugian moral, tetapi juga trauma psikologis yang mendalam karena citranya digunakan tanpa izin. Oleh karena itu, negara harus menjamin hak korban untuk mendapatkan pemulihan yang layak. Pemulihan tersebut mencakup hak untuk menghapus konten yang tersebar, memperoleh kompensasi moral maupun material, serta mendapatkan bantuan hukum dan psikologis. Perlindungan terhadap korban juga perlu diperluas ke ranah digital, misalnya dengan mewajibkan penyedia layanan internet bekerja sama dengan lembaga penegak hukum dalam melakukan pelacakan dan penghapusan konten yang merugikan.

Selanjutnya, sistem hukum pidana harus bergerak ke arah yang lebih preventif dan adaptif. Dalam era digital, mencegah kejahatan jauh lebih efektif dibandingkan menindak setelah kerugian terjadi. Pemerintah dapat mengembangkan sistem verifikasi konten digital berbasis *blockchain* atau tanda air digital (*digital watermarking*) untuk memastikan keaslian dan integritas video maupun gambar yang beredar di internet. Teknologi ini tidak hanya membantu proses pembuktian dalam ranah hukum, tetapi juga menjadi upaya preventif dalam mengurangi penyebaran konten palsu. Misalnya, setiap video yang diunggah ke platform dapat secara otomatis diberi tanda autentikasi yang mencatat asal, waktu, dan perangkat pembuatannya. Dengan demikian, apabila muncul konten yang mencurigakan, proses identifikasi dapat dilakukan lebih cepat dan akurat.

Namun, pembaruan hukum pidana tidak boleh hanya berfokus pada aspek teknis atau penambahan aturan semata. Hal yang jauh lebih penting adalah perubahan paradigma penegakan hukum itu sendiri. Hukum harus dipahami sebagai bagian dari sistem sosial yang dinamis, bukan sekadar alat negara untuk menghukum. Dalam konteks ini, penegakan hukum perlu diarahkan

[11] Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). *Deepfakes: Trick or Treat?* Business Horizons, 63(2), 135–146.

DOI: https://doi.org/10.62017/merdeka

pada penciptaan rasa aman dan adil bagi masyarakat, serta mampu menumbuhkan kesadaran etis di dunia digital. Pendidikan hukum dan literasi digital bagi masyarakat luas harus menjadi bagian dari strategi besar penanggulangan kejahatan berbasis AI. Masyarakat yang paham akan risiko *deepfake* dan cara melindungi data pribadinya akan menjadi lapisan pertahanan pertama dalam menghadapi ancaman siber.

Selain itu, kolaborasi antarinstansi juga menjadi kunci. Lembaga penegak hukum seperti kepolisian, kejaksaan, dan pengadilan perlu bekerja sama dengan kementerian yang membidangi komunikasi dan teknologi, serta sektor swasta penyedia layanan digital. Tanpa kerja sama lintas sektor, upaya menghadapi kejahatan digital hanya akan bersifat tambal sulam. Negara juga perlu menyiapkan aparat penegak hukum yang memiliki kompetensi teknologis memadai agar dapat memahami mekanisme kerja AI dan cara pembuktian kejahatan digital secara ilmiah. Dengan demikian, proses penegakan hukum tidak lagi tertinggal dari modus kejahatan yang terus berevolusi.

Akhirnya, arah pembaruan hukum pidana yang ideal bukan hanya menambah pasal-pasal baru, tetapi juga menata ulang filosofi hukum pidana itu sendiri. Hukum harus dilihat sebagai instrumen yang melindungi manusia dari dampak negatif kemajuan teknologi, bukan sekadar sebagai alat penjeraan. Prinsip kepastian hukum, keadilan, dan kemanfaatan harus dijaga seimbang, sementara perlindungan terhadap hak asasi manusia tetap menjadi prioritas utama. Dalam menghadapi tantangan era digital yang kompleks, hukum pidana Indonesia dituntut untuk lebih progresif, visioner, dan responsif terhadap perubahan zaman. Dengan demikian, pembaruan hukum yang adaptif akan memastikan bahwa kemajuan teknologi tetap berpihak pada kemanusiaan, bukan sebaliknya menjadi ancaman bagi martabat dan kebebasan individu.

KESIMPULAN

Fenomena *deepfake pornography* merupakan wujud nyata dari tantangan hukum pidana di era kecerdasan buatan (*Artificial Intelligence/AI*) yang berkembang pesat, namun belum sepenuhnya terjangkau oleh sistem hukum nasional. Berdasarkan hasil analisis yuridis terhadap KUHP dan UU ITE, dapat disimpulkan bahwa Indonesia saat ini menghadapi kekosongan norma hukum (legal vacuum) yang serius dalam menanggulangi kejahatan berbasis manipulasi digital ini. KUHP masih berpijak pada paradigma kejahatan konvensional yang mensyaratkan adanya tindakan cabul secara fisik, sedangkan UU ITE hanya menekankan aspek distribusi konten tanpa menyentuh substansi rekayasa digital sebagai bagian dari tindak pidana. Akibatnya, pelaku *deepfake pornography* sulit dijerat hukum, sementara korban tidak memperoleh perlindungan yang memadai terhadap pelanggaran privasi dan kehormatan mereka.

Dari sisi penegakan hukum, keterbatasan kemampuan *digital forensics*, lemahnya koordinasi antarinstansi, serta absennya mekanisme tanggung jawab bagi platform digital memperparah kondisi tersebut. Hal ini menyebabkan keadilan substantif bagi korban semakin sulit tercapai, sekaligus memperlihatkan ketertinggalan sistem hukum pidana Indonesia dalam merespons dinamika kejahatan digital global. Sementara di negara-negara seperti Amerika Serikat, Korea Selatan, dan Inggris, *deepfake pornography* telah diatur secara tegas melalui undang-undang khusus yang mengakui tindakan manipulasi digital tanpa persetujuan sebagai bentuk kejahatan serius terhadap privasi dan kesusilaan.

Dengan demikian, arah pembaruan hukum pidana yang ideal di Indonesia harus diarahkan pada tiga hal utama. Pertama, perumusan norma hukum baru yang secara eksplisit mengatur kejahatan berbasis AI, termasuk definisi *deepfake*, unsur delik, serta tanggung jawab pidana bagi pembuat, penyebar, dan pihak yang memanfaatkan konten tersebut. Kedua, penguatan perlindungan terhadap hak privasi dan martabat manusia melalui instrumen hukum pidana dan kebijakan teknologi yang berpihak pada korban. Ketiga, transformasi paradigma penegakan hukum dari yang bersifat reaktif menjadi preventif, dengan mengintegrasikan teknologi pendeteksi konten palsu dan sistem kerja sama lintas lembaga untuk memperkuat pembuktian dan perlindungan digital.

Hukum pidana harus kembali pada fungsinya sebagai alat perlindungan masyarakat dan penjaga keadilan di tengah kemajuan teknologi. Reformasi hukum yang berbasis pada prinsip

keadilan, kemanusiaan, dan adaptasi terhadap inovasi digital merupakan langkah mutlak agar Indonesia tidak hanya menjadi penonton dalam menghadapi revolusi teknologi, tetapi juga menjadi negara hukum yang tangguh, responsif, dan berkeadilan di era kecerdasan buatan.

DAFTAR PUSTAKA

Chesney, R., & Citron, D. K. (2019). *Deep Fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107*(6), 1753–1820. https://doi.org/10.2139/ssrn.3213954

Chesney, R., & Citron, D. K. (2019). *Deep Fakes and the new disinformation war: The coming age of post-truth geopolitics. Foreign Affairs, 98*(1), 147–155.

Deeptrace. (2019). *The State of Deepfakes: Landscape, threats, and impact.* Amsterdam: Deeptrace Labs. https://www.deeptracelabs.com/reports

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). *Deepfakes: Trick or treat? Business Horizons, 63*(2), 135–146. https://doi.org/10.1016/j.bushor.2019.11.006

Mahendra, A. (2023). *Analisis yuridis terhadap kejahatan siber dan kekosongan norma dalam UU ITE. Jurnal Hukum Teknologi, 8*(2), 112–128.

Muladi. (2021). *Hukum pidana dan perkembangan teknologi informasi.* Bandung: Alumni.

Setiadi, H. (2024). *Forensik digital dalam pembuktian tindak pidana siber. Jurnal Ilmu Hukum dan Teknologi, 6*(1), 75–89.

Setiadi, W. (2023). *Tantangan hukum siber di Indonesia dalam menghadapi kejahatan deepfake. Jurnal Hukum & Teknologi, 8*(1), 44–59.

Simanjuntak, P. (2022). *Kejahatan digital dan kekosongan norma hukum pidana Indonesia. Jurnal Ilmu Hukum Lex Renaissance, 7*(2), 201–218.