



Pemidanaan Kepada Pelaku Konten Pornografi Menggunakan Aplikasi *Deepfake* Pada Peraturan Perundang-Undangan di Indonesia

Sholahudin Jagad Al-Ayoubi^{1*}, Miko Aditiya Suharto²

¹UPN “Veteran” Jawa Timur, Surabaya, Indonesia

²UPN “Veteran” Jawa Timur, Surabaya, Indonesia

*Corresponding Author: sholahudinjagad@gmail.com

Artikel Histori

Direvisi: 16-08-2025

Diterima: 05-09-2025

Diterbitkan: 17-09-2025

Abstrak: Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence/AI*) telah melahirkan inovasi baru dalam bentuk *deepfake*, yaitu teknologi manipulasi wajah yang mampu menciptakan konten visual palsu secara meyakinkan. Salah satu penyalahgunaan teknologi ini adalah dalam pembuatan dan penyebaran konten pornografi, yang dapat merusak reputasi, privasi, serta martabat korban, meskipun mereka tidak pernah benar-benar terlibat dalam pembuatan konten tersebut. Studi ini berfokus pada pengkajian bentuk pemidanaan yang dapat dikenakan terhadap individu yang menyebarkan konten pornografi yang dihasilkan melalui teknologi *deepfake*, dalam kerangka hukum pidana nasional, khususnya merujuk pada ketentuan yang diatur dalam UU No. 44/2008 tentang Pornografi. Penelitian dilaksanakan dengan menggunakan pendekatan yuridis normatif, melalui telaah terhadap peraturan perundang-undangan serta kajian literatur yang sesuai. Temuan dari penelitian ini memperlihatkan bahwa meskipun hingga seakrang ini belum didapati ketentuan hukum yang eksplisit mengatur tentang penggunaan teknologi *deepfake*, namun penenaan sanksi pidana terhadap perbuatan tersebut masih dimungkinkan melalui konstruksi norma yang telah ada. Pelaku dapat dikenakan sanksi berdasarkan UU Pornografi, UU ITE, serta UU PDP. Namun, masih terdapat tantangan dalam aspek pembuktian dan pelacakan digital, yang menuntut reformasi hukum dan peningkatan kapasitas penegak hukum. Oleh karena itu, pengaturan yang lebih spesifik mengenai *deepfake* perlu segera dihadirkan dalam sistem hukum nasional Indonesia.

Kata Kunci: Tindak Pidana, Pornografi, *Deepfake*

Abstract: The advancement of Artificial Intelligence (AI) technology has led to the emergence of *deepfake*, a facial manipulation innovation capable of creating convincingly fake visual content. One of the most concerning misuses of this technology is the creation and distribution of pornographic content, which can severely damage the reputation, privacy, and dignity of victims, even though they were never truly involved in the production of such material. This study focuses on analyzing the criminal liability that can be imposed on individuals who disseminate pornographic content generated through *deepfake* technology within the framework of Indonesian criminal law, particularly referring to the provisions outlined in Law Number 44 of 2008 on Pornography. The research employs a normative juridical approach, by reviewing relevant legislation and academic literature. The findings reveal that although there is currently no specific regulation addressing the use of *deepfake* technology, criminal sanctions may still be imposed through the interpretation and application of existing legal norms. Perpetrators may be held accountable under the Pornography Law, the Electronic Information and Transactions (ITE) Law, and the Personal Data Protection (PDP) Law. However, challenges persist, especially in the areas of digital evidence collection and perpetrator identification, which necessitate legal reform and improved law enforcement capacity. Therefore, the urgent need for more specific

regulation on deepfake should be addressed within Indonesia's national legal framework.

Keywords: Criminalization, Pornography, Deepfake

PENDAHULUAN

AI adalah teknologi untuk meniru kecerdasan manusia dengan tujuan mempermudah dalam proses pengambilan data yang diminta berdasarkan kumpulan data yang sudah diberikan. Kecerdasan Buatan (Artificial Intelligence/AI) pertama kali diperkenalkan pada tahun 1950 oleh Alan Turing, yang merancang konsep dasar dari sistem yang kini dikenal sebagai AI. Kemudian, pengembangan lebih lanjut terhadap konsep ini dilakukan oleh John McCarthy pada tahun 1956. Pada dekade 1980-an, teknologi AI mulai diperkenalkan di Indonesia dan swlanjutnya selalu mengalami adanya peningkatan secara bertahap dengan kecepatan yang tidak bisa diremehkan. AI dipahami sebagai hasil pengembangan dari sistem komputer yang dirancang untuk melaksanakan tugas-tugas yang sebelumnya secara eksklusif dilakukan oleh manusia. Dalam praktiknya, sejumlah istilah telah dikaitkan erat dengan AI, seperti *machine learning*, *deep learning*, *Artificial Neural Network* (ANN) atau jaringan saraf tiruan, serta *Natural Language Processing* (NLP) atau pemrosesan bahasa alami.¹ Penerapan AI telah menghasilkan sesuatu yang baru dan secara signifikan terhadap berbagai sektor industri, misalnya teknologi pengenalan audio dan visual, kendaraan otonomis, hingga layanan di bidang kesehatan. Bahkan, saat ini AI telah dimanfaatkan secara langsung oleh individu sebagai alat untuk mengoptimalkan keuntungan pribadi dalam sektor bisnis, yang menunjukkan bahwa pemanfaatan teknologi ini telah meluas melampaui kepentingan korporasi besar dan menyentuh ranah privat.²

Seiring berjalannya waktu, AI dapat memberikan ancaman yang lebih besar ketika terdapat pihak yang menggunakan varian baru AI yang berpotensi melanggar etika. Keberadaan AI yang bebas dapat digunakan untuk membuat disinformasi yang lebih meyakinkan, memproduksi lebih banyak konten palsu secara masif, bahkan dapat mengubahnya menjadi alat yang memindai sosial media yang menjurus kepada provokatif. Teknologi yang dapat digunakan untuk membuat sekaligus memanipulasi konten berbentuk gambar, suara, dan video yang realistis disebut sebagai *Deepfake*. Istilah *Deepfake* muncul pada 2017 oleh pengguna *reddit* yang merupakan seorang *anonym* untuk teknologi yang menggunakan *Deeplearning* untuk melatih program komputer dalam mengumpulkan data video seseorang. Program ini selanjutnya melakukan peniruan ekspresi wajah dan Gerakan hingga menjadikannya video palsu.³ Teknologi *Deepfake*, pada hakikatnya, dipandang layaknya pedang bermata dua. Di satu sisi, kemudahan dalam menyelesaikan berbagai pekerjaan telah dihadirkan oleh teknologi ini; namun di sisi lain, potensi ancaman yang ditimbulkannya juga menasar ketertiban sosial serta keamanan negara dan tidak hanya terfokus pada individu saja. Hampir di seluruh sektor seperti politik, ekonomi, maupun dalam hal pelanggaran asusila seperti pornografi, penyalahgunaan teknologi *Deepfake* telah dilakukan secara masif.

Secara definisi, *cybercrime* dapat dipahami sebagai tindak kejahatan yang melibatkan perangkat komputer sebagai alat untuk melakukan pelanggaran terhadap hukum. Kemunculan kejahatan ini tidak terlepas dari kemajuan pesat di bidang teknologi digital, terutama yang berkaitan dengan dunia maya. Fenomena ini memiliki akar historis yang panjang dan dapat ditelusuri hingga awal abad ke-20, ketika praktik *hacking* pertama kali terjadi. Misalnya,

¹ Fadhilah, a. D. Z., & Retnoningsih, s. (2024). Perancangan kampanye digital melawan disinformasi melalui artificial intelligence dan *Deepfake* di kalangan pra lansia usia 45-55 tahun. *Fad*, 3(02).

² Ibid

³ Situmeang, B. S., Dkk. (2024). Pengaruh *Artificial Intelligence* Terhadap Tingkat Kasus *Deepfake* Pada Selebritas di Twitter. *Device*, 14(1).

pada dekade 1870-an, terdapat kasus di mana sekelompok remaja mengganggu sistem telepon yang baru dibangun dengan cara memanipulasi otoritas sistem tersebut. Selanjutnya, pada dekade 1960-an, istilah *hacker* awalnya tidak memiliki konotasi negatif, melainkan digunakan untuk menyebut individu yang memiliki keahlian tinggi dalam bidang komputer. Di masa itu, sejumlah institusi pendidikan seperti MIT (*Massachusetts Institute of Technology*) telah menjadi tempat berkembangnya eksperimen terhadap sistem komputer besar, termasuk laboratorium kecerdasan buatan, yang turut menjadi wadah bagi para hacker untuk menguji kemampuan mereka dalam menciptakan program-program di luar kapasitas standar yang dirancang untuk perangkat tersebut

Pornografi berbasis *deepfake* adalah sebuah bentuk penyalahgunaan teknologi AI yang paling meresahkan karena menyerang aspek privasi, martabat, dan integritas individu terutama perempuan. Teknologi *deepfake* memungkinkan seseorang untuk membuat video pornografi palsu yang menampilkan wajah orang lain, biasanya tokoh publik atau bahkan individu biasa, yang sebenarnya tidak pernah terlibat dalam adegan tersebut. *Deepfake* pornografi tidak hanya menasar tokoh terkenal. Banyak perempuan biasa, termasuk jurnalis, aktivis, dan pelajar, menjadi korban setelah wajah mereka diambil dari media sosial lalu dimanipulasi ke dalam konten pornografi palsu. Salah satu laporan dari Deeptrace, sebuah lembaga riset keamanan siber, menunjukkan bahwa pada tahun 2019, 96% dari semua video *deepfake* yang beredar di internet adalah pornografi, dan hampir seluruhnya menargetkan perempuan.⁴

Dalam konteks hukum Indonesia, perbuatan memproduksi atau menyebarkan konten pornografi merupakan pelanggaran terhadap Undang-Undang Nomor 44/2008 tentang Pornografi, yang secara tegas mengatur larangan pembuatan, penyebaran, dan kepemilikan materi pornografi. Pasal 4 ayat (1) Undang-Undang Pornografi mengatur bahwa setiap individu dilarang untuk terlibat dalam segala bentuk kegiatan yang berkaitan dengan pornografi, termasuk di dalamnya tindakan memproduksi, menciptakan, memperbanyak, mendistribusikan, menyiarkan, mengimpor, mengeksport, memperdagangkan, menyewakan, menawarkan, atau menyediakan materi bermuatan pornografi dalam bentuk apa pun. Pelaku yang memanipulasi konten visual dengan mengganti wajah seseorang melalui *deepfake* untuk tujuan pornografi jelas termasuk dalam kategori pelanggaran ini.

Namun, penerapan pidana terhadap pelaku kejahatan berbasis *deepfake* masih menghadapi tantangan. Hal ini disebabkan belum adanya regulasi khusus yang secara eksplisit mengatur tentang kejahatan berbasis AI, termasuk *deepfake*. Akibatnya, aparat penegak hukum kerap mengalami kendala dalam menetapkan dasar pidana yang tepat. Di samping itu, pendekatan konvensional dalam UU Pornografi belum sepenuhnya mampu mengakomodasi kompleksitas dan modus operandi kejahatan berbasis teknologi ini.

Kondisi ini menciptakan urgensi untuk meninjau kembali efektivitas dan kecukupan regulasi yang ada, serta pentingnya memberikan pidana yang tegas kepada pelaku penyebaran konten pornografi dengan teknologi *deepfake*. Penelitian ini bertujuan untuk menganalisis pidana terhadap pelaku penyalahgunaan teknologi *deepfake* untuk konten pornografi dalam kerangka UU Pornografi, serta mengidentifikasi celah hukum yang mungkin timbul dalam praktik penegakan hukum terhadap fenomena tersebut.

METODE

Penelitian ini dilakukan dengan menggunakan metode yuridis normatif, yang mengkaji permasalahan hukum melalui pendekatan peraturan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), serta pendekatan studi kasus (*case study*).

⁴ Deeptrace (2019), "The State of Deepfakes: Landscape, Threats and Impact." https://regmedia.co.uk/2019/10/08/deepfake_report.pdf Diakses pada 25 Mei 2025

Dalam proses pengumpulan dan analisis data, penelitian ini mengandalkan berbagai sumber bahan hukum, meliputi bahan hukum primer, sekunder, serta bahan non-hukum yang relevan untuk memperkuat argumentasi.

HASIL DAN PEMBAHASAN

Pertanggungjawaban Pidana Pelaku Pornografi Pada *Cyber Space* Dalam Peraturan Perundang-Undangan di Indonesia

Pornografi berbasis *deepfake* merupakan salah satu bentuk penyalahgunaan teknologi kecerdasan buatan yang paling meresahkan karena menyerang aspek privasi, martabat, dan integritas individu terutama perempuan. Teknologi *deepfake* memungkinkan seseorang untuk membuat video pornografi palsu yang menampilkan wajah orang lain, biasanya tokoh publik atau bahkan individu biasa, yang sebenarnya tidak pernah terlibat dalam adegan tersebut. Dengan hanya menggunakan beberapa foto dari media sosial, algoritma *deep learning* dapat "menempelkan" wajah korban ke tubuh orang lain dalam video porno secara sangat realistis, sehingga hasil akhirnya terlihat seperti asli. Lebih mencemaskan lagi, *deepfake* pornografi tidak hanya menysar tokoh terkenal. Banyak perempuan biasa, termasuk jurnalis, aktivis, dan pelajar, menjadi korban setelah wajah mereka diambil dari media sosial lalu dimanipulasi ke dalam konten pornografi palsu. Ini menunjukkan bahwa pornografi *deepfake* bukan hanya masalah teknologi, tetapi juga berkaitan erat dengan isu gender, kekuasaan, dan kekerasan berbasis digital.⁵ Terdapat beberapa pengaturan di Indonesia yang dapat dikenakan terhadap seseorang yang melakukan kejahatan menggunakan *Deepfake*.

a. UU Pornografi (UU Nomor 4 Tahun 2008)

Dalam Pasal 1 angka 1 UU No. 44/2008 tentang Pornografi, dijelaskan bahwa segala bentuk media, baik berupa gambar, sketsa, ilustrasi, foto, tulisan, suara, bunyi, gambar bergerak, animasi, kartun, percakapan, gerakan tubuh, maupun bentuk penyampaian pesan lainnya yang disalurkan melalui berbagai sarana komunikasi atau dipertunjukkan di ruang publik dan memuat unsur cabul atau eksploitasi seksual, dikategorikan sebagai pornografi. Dalam konteks ini, konten *deepfake* yang memperlihatkan wajah seseorang seolah-olah sedang melakukan tindakan seksual, meskipun hasil manipulasi teknologi, dapat diklasifikasikan sebagai "gambar bergerak" atau "animasi bermuatan cabul." Dengan demikian, konten semacam itu termasuk dalam ruang lingkup yang diatur oleh UU Pornografi. Hal ini diperkuat dengan ketentuan dalam Pasal 4 ayat (1) undang-undang yang sama, yang secara tegas melarang setiap individu untuk memproduksi, menciptakan, memperbanyak, menggandakan, menyebarkan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan materi pornografi dalam bentuk apapun.⁶ Pasal ini menyebutkan, dalam hal ini ppidanaannya diatur pada pasal 29 mengatur larangan terhadap tindakan yang melibatkan peredaran dan produksi konten bermuatan pornografi. pasal ini menitikberatkan pada dua unsur utama, yakni unsur kesengajaan dan objek yang tergolong pornografi. Kesengajaan di sini mencakup adanya niat (*dolus*) dan kehendak sadar pelaku untuk melakukan perbuatan yang dilarang oleh undang-undang. Hal ini menjadi kunci dalam menegakkan unsur subjektif tindak pidana. Sedangkan unsur objektifnya merujuk pada tindakan konkret dalam bentuk produksi maupun distribusi konten yang tergolong pornografi. Dalam konteks perkembangan teknologi informasi dan komunikasi, penggunaan *deepfake* sebagai alat untuk memproduksi konten pornografi menimbulkan dimensi baru dalam interpretasi hukum. *Deepfake* memungkinkan penciptaan citra atau video fiktif yang menyerupai

⁵ Ibid

⁶ UU No. 44/2008 tentang Pornografi

orang sungguhan, seolah-olah individu tersebut melakukan perbuatan seksual atau tindakan yang bersifat asusila. Walaupun konten tersebut bersifat hasil manipulasi digital, esensi dari muatannya tetap masuk dalam kategori pornografi sebagaimana diatur oleh undang-undang. Hal ini menjadi kunci dalam menegakkan unsur subjektif tindak pidana. Sedangkan unsur objektifnya merujuk pada tindakan konkret dalam bentuk produksi maupun distribusi konten yang tergolong pornografi. Dalam konteks perkembangan teknologi informasi dan komunikasi, penggunaan *deepfake* sebagai alat untuk memproduksi konten pornografi menimbulkan dimensi baru dalam interpretasi hukum. *Deepfake* memungkinkan penciptaan citra atau video fiktif yang menyerupai orang sungguhan, seolah-olah individu tersebut melakukan perbuatan seksual atau tindakan yang bersifat asusila. Walaupun konten tersebut bersifat hasil manipulasi digital, esensi dari muatannya tetap masuk dalam kategori pornografi sebagaimana diatur oleh undang-undang. Dengan demikian, seseorang yang menggunakan teknologi *deepfake* untuk menciptakan atau menyebarkan konten tersebut tetap dapat dimintai pertanggungjawaban pidana berdasarkan Pasal 29 UU Pornografi, sejauh terpenuhinya unsur kesengajaan dan sifat pornografis konten tersebut.

Pada Pasal 27 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (yang telah diubah dengan UU No. 19 Tahun 2016) juga mengatur larangan distribusi konten yang melanggar kesusilaan melalui sistem elektronik, Pasal 29 UU Pornografi memberikan dasar hukum yang lebih detail. UU Pornografi secara khusus mengatur mengenai definisi dan cakupan pornografi, termasuk bentuk-bentuknya yang tidak hanya terbatas pada media elektronik. Oleh karena itu, penerapan Pasal ini dalam konteks kejahatan menggunakan teknologi *deepfake* memberikan pendekatan hukum yang lebih tepat karena menasar pada substansi dan bentuk konten, tidak hanya pada medium penyebarannya.

Pasal tersebut juga menyebutkan bahwa seseorang yang terbukti bersalah dalam hal ini melakukan hal hal yang dilarang dalam pasal tersebut, dapat dikenakan pidana berupa pidana penjara dengan durasi paling singkat 6 (enam) bulan dan paling lama 12 (dua belas) tahun dengan tambahan pidana denda paling sedikit Rp. 250.000.000,00 (dua ratus lima puluh juta rupiah) dan paling banyak Rp. 6.000.000.000,00 (enam miliar rupiah). Dengan demikian, apabila seseorang terbukti secara sengaja menyebarkan konten *deepfake* yang bermuatan pornografi, maka pelaku dapat dikenakan pidana berdasarkan pasal ini, karena telah melanggar ketentuan yang melarang penyebaran muatan yang melanggar kesusilaan melalui media elektronik.

b. UU Informasi dan Transaksi Elektronik (UU Nomor 11 Tahun 2008)

Salah satu dasar hukum utama yang relevan adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Undang-undang ini, meskipun tidak menyebut AI secara langsung, memiliki cakupan yang cukup luas dalam mengatur perilaku di dunia maya. Ketentuan dalam UU ITE dapat digunakan untuk menindak pelaku yang menggunakan AI untuk melakukan tindak pidana, seperti penyebaran hoaks, pencemaran nama baik, penipuan digital, atau pelanggaran terhadap norma sosial, termasuk melalui teknologi seperti *deepfake*. Pada pasal 27 ayat (1) dapat dilihat dari salah satu konten *deepfake* yang sempat viral baru baru ini yaitu salah satu mahasiswa dari universitas negeri di Bali yang membuat konten pornografi dengan menggunakan foto instagram dari 35 mahasiswi lain untuk disebarluaskan dengan aplikasi telegram.⁷ Kasus tersebut dapat menjadi contoh

⁷ Ginta Y.V.S. dan Hartik A. (2025), Mahasiswa Universitas Udayana Bali Diduga Bikin Konten Porno Palsu Berbasis AI. <https://denpasar.kompas.com/read/2025/04/25/131021978/mahasiswa-universitas-udayana-bali-diduga-bikin-konten-porno-palsu-berbasis> Diakses pada 22 Mei 2025

bahwa deepfake dapat digunakan untuk melakukan kejahatan kesusilaan dengan mengubah wajah orang lain pada konten asusila dengan orang yang terkenal.

Dalam konteks kejahatan yang melibatkan teknologi deepfake, pasal ini menjadi sangat relevan. Deepfake, sebagai sebuah teknologi berbasis kecerdasan buatan, memungkinkan manipulasi citra dan video secara realistis sehingga dapat menciptakan konten pornografi sintesis yang seolah-olah menampilkan seseorang dalam adegan seksual, meskipun orang tersebut sama sekali tidak pernah terlibat. Konten semacam ini jelas mengandung muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal tersebut, karena menyerang nilai-nilai moral dan norma kesopanan yang berlaku di masyarakat.

Pada pasal tersebut menggunakan frasa “dengan sengaja” dan “tanpa” hak” mengisyaratkan bahwa perbuatan yang dimaksud akan menjadi suatu tindak pidana jika seseorang berkehendak untuk melakukan hal tersebut dan jika hal tersebut terjadi karena kelalaiannya maka tidak akan menjadi suatu tindak pidana. Makna “dengan sengaja” itu juga memperluas cakupan dari pasal tersebut karena dalam hukum pidana, “sengaja” dibedakan menjadi 3 bagian yaitu sengaja dengan maksud, sengaja dengan kesadaran kepastian dan sengaja dengan kesadaran kemungkinan.⁸ Selanjutnya pada frasa “tanpa hak” yang terletak pada pasal ini sendiri menerangkan bahwa seseorang memiliki hak dalam melakukan hal tersebut dan tidak akan dipidana jika memang memiliki hak dalam melakukan hal tersebut. Unsur berikutnya adalah “menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya” pada pasal tersebut dan “mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya”. Pelaku yang membuat dan menyebarluaskan konten deepfake pornografi dapat dikualifikasikan telah memenuhi unsur tindak pidana sebagaimana dimaksud dalam pasal tersebut, yaitu unsur kesengajaan, tanpa hak, serta muatan yang bersifat melanggar kesusilaan. Apalagi, dalam praktiknya, pelaku umumnya tidak mendapatkan izin dari orang yang wajah atau tubuhnya direkayasa dalam video tersebut. Oleh karena itu, meskipun UU ITE tidak secara khusus menyebut istilah deepfake, ruang lingkup norma dalam Pasal tersebut tetap dapat menjangkau tindak pidana tersebut melalui interpretasi hukum berdasarkan muatan kesusilaannya.

Terhadap pelanggaran pasal ini, sanksi pidana diatur dalam Pasal 45 ayat (1) UU ITE, yang menyebutkan bahwa pelaku dapat dikenakan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Dengan demikian, apabila seseorang terbukti secara sengaja menyebarkan konten deepfake yang bermuatan pornografi, maka pelaku dapat dikenakan pemidanaan berdasarkan pasal ini, karena telah melanggar ketentuan yang melarang penyebaran muatan yang melanggar kesusilaan melalui media elektronik.

c. UU Perlindungan data Pribadi (UU Nomor 27 tahun 2022)

Pasal 67 ayat (1) Undang-Undang No. 27/2022 tentang Perlindungan Data Pribadi memuat ketentuan pidana terhadap siapa pun yang dengan sengaja dan tanpa hak menggunakan data pribadi milik orang lain. Ketentuan ini mencerminkan perlindungan hukum terhadap hak individu atas kendali dan otoritas terhadap informasi pribadinya. Dalam era digital yang serba terkoneksi, data pribadi seperti nama, gambar, video, wajah, suara, hingga informasi biometrik lainnya dapat dengan mudah dikumpulkan, disimpan, dan disalahgunakan oleh pihak lain untuk berbagai kepentingan, termasuk yang melanggar hukum. Dalam kaitannya dengan kejahatan digital seperti deepfake, pasal ini menjadi sangat relevan. Teknologi deepfake bekerja dengan cara merekayasa visual, seperti

⁸ Suseno S., (2012), *Yurisdiksi tindak pidana siber*, Bandung: Refika Aditama

mengganti wajah seseorang di dalam sebuah video dengan wajah orang lain, sehingga tampak nyata. Jika wajah seseorang digunakan tanpa izin untuk membuat konten manipulatif terutama konten yang bermuatan asusila atau pornografi maka penggunaan data pribadinya tersebut sudah termasuk sebagai pelanggaran terhadap Pasal tersebut. Dalam hal ini, wajah merupakan bagian dari identitas pribadi yang dilindungi undang-undang, sehingga siapa pun yang mengakses dan memakainya tanpa persetujuan pemiliknya telah melakukan pelanggaran.

Dalam konteks pornografi berbasis *deepfake*, pasal ini sangat relevan karena pelaku biasanya mengakses, mengambil, atau mengumpulkan data pribadi milik orang lain seperti foto, video, atau data biometrik (misalnya wajah dan suara) tanpa izin. Data tersebut kemudian dimanipulasi dengan teknologi kecerdasan buatan untuk menciptakan konten pornografi seolah-olah melibatkan individu yang datanya dicuri. Perbuatan ini jelas merupakan bentuk perolehan data pribadi secara melawan hukum dan dilakukan untuk keuntungan pribadi (baik dalam bentuk ekonomi, ketenaran, atau kepuasan pribadi), serta menimbulkan kerugian nyata bagi subjek data, seperti kerusakan nama baik, gangguan psikologis, dan kerugian sosial.

Dengan demikian, Pasal tersebut menerangkan bahwa sanksi pidana diatur langsung dalam pasal yang sama, yang menyebutkan bahwa pelaku dapat dikenakan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). Dengan demikian, apabila seseorang secara sengaja dan tanpa hak memperoleh atau mengumpulkan data pribadi orang lain seperti foto wajah, suara, atau rekaman video untuk digunakan dalam pembuatan konten *deepfake* yang bermuatan pornografi, maka perbuatan tersebut dapat dijerat dengan ketentuan ini. Tindakan tersebut memenuhi unsur memperoleh data pribadi secara melawan hukum, dengan maksud memperoleh keuntungan, dan telah menimbulkan kerugian bagi subjek data. Oleh karena itu, Pasal tersebut memberikan landasan pemidanaan yang tegas terhadap penyalahgunaan data pribadi dalam konteks kejahatan pornografi digital berbasis teknologi kecerdasan buatan seperti *deepfake*.

Tantangan Dalam Penanganan Kasus Pornografi Menggunakan *Deepfake*

Penegakan hukum terhadap *deepfake* pornografi di Indonesia menghadapi kekosongan regulasi (*legal vacuum*). Pasal 1 ayat (1) KUHP (asas legalitas) mensyaratkan ada aturan yang jelas untuk menetapkan suatu perbuatan sebagai tindak pidana. Saat ini belum ada ketentuan khusus yang secara eksplisit mengatur pembuatan atau penyebaran konten pornografi *deepfake*, sehingga terjadi ketidakpastian hukum. Berbagai kajian menyebutkan bahwa ketiadaan regulasi khusus tersebut menimbulkan tantangan besar bagi penegakan hukum dan perlindungan korban.⁹ Sebagai contoh, studi menyatakan bahwa belum memiliki peraturan komprehensif yang mengatur teknologi *deepfake* dan meski *deepfake* pornografi dapat dikaitkan dengan UU ITE, UU Pornografi, dan UU PDP, belum ada payung hukum khusus untuk mengatur dan memberi sanksi yang tegas.¹⁰

Secara normatif, aparat penegak hukum saat ini menjerat kasus *deepfake* pornografi berdasarkan ketentuan dalam hukum positif yang ada. Misalnya Undang-Undang No.44/2008 tentang Pornografi mengatur larangan produksi dan penyebaran materi pornografi.¹¹ Undang-Undang No. 11/2008 jo. No. 19/2016 tentang ITE melarang penyebaran

⁹ Arvitto R. (2024). Implikasi Hukum *Deepfake*: Telaah terhadap UU ITE dan UU PDP. 4.2 73-82

¹⁰ Patikasari, T. *Pelindungan Hukum Bagi Korban Deepfake Pornografi (Studi Perbandingan Indonesia dan Korea Selatan)* (Bachelor's thesis, Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta).

¹¹ Ferdinal, O., & Bakir, H. (2024). Legal Protection Efforts and Policies to Combat *Deepfake* Porn Crimes with Artificial Intelligence (AI) in Indonesia. *Journal of Multidisciplinary Sustainability Asean*, 1(6), 465-474.

informasi elektronik yang bermuatan pornografi (Pasal 27 ayat 1 dan 3 UU ITE) dan pencemaran nama baik secara elektronik, sehingga dalam praktik dapat digunakan untuk menjerat pelaku *deepfake* yang memuat wajah korban tanpa izin.¹² Undang-Undang No. 27/2022 tentang Perlindungan Data Pribadi dapat dipakai untuk menjerat pelaku yang menyalahgunakan data pribadi (wajah) korban. Namun, karena tidak ada pasal khusus menyebut “*deepfake*”, penerapan hukum tersebut seringkali bersifat interpretatif dan belum teruji pengadilan. Sebagaimana diungkapkan, UU ITE yang dimiliki oleh Indonesia sekarang ini belum sepenuhnya mengakomodir pelaku pembuatan video *deepfake* pornografi dan kekurangan aturan jelas tentang *deepfake* menimbulkan ketidakpastian hukum.¹³ Situasi ini memperkuat rasa tidak yakin aparat dalam menjatuhkan sanksi sesuai asas legalitas (*nullum crimen sine lege*).

Dari sudut teknis, aparat penegak hukum di Indonesia menghadapi keterbatasan kemampuan dan sarana dalam menghadapi kejahatan *deepfake*. Deteksi *deepfake* membutuhkan teknologi dan keahlian tinggi yang saat ini belum dimiliki secara memadai oleh banyak penyidik. Studi menunjukkan bahwa untuk mendeteksi dan membuktikan manipulasi AI *deepfake* diperlukan alat forensik digital dan pemahaman teknis mendalam tentang AI dan citra digital.¹⁴ Namun aparat penegak hukum kita umumnya belum tersertifikasi dalam keahlian ini. Sehingga Polisi/kejaksaan sering kekurangan perangkat lunak analisis citra atau laboratorium forensik khusus yang memadai.¹⁵ Kondisi ini mengakibatkan keterlambatan atau ketidaktepatan saat investigasi.

Kurangnya infrastruktur forensik digital juga menjadi kendala. Indonesia belum memiliki laboratorium forensik di setiap daerah, sehingga sampel digital sering diantar jauh ke Puslabfor Bareskrim Polri atau Balai Besar. Proses validasi bukti *deepfake* pun menuntut komputasi berat misalnya memeriksa ribuan detik video atau foto untuk menemukan distorsi halus hasil AI.¹⁶ Padahal penyidik perlu segera mengamankan bukti sebelum terhapus. Semua ini menuntut investasi besar dalam fasilitas forensik, namun sejauh ini masih minim.

Pelatihan SDM juga menjadi isu penting. Rendahnya pemahaman personel hukum tentang AI membuat mereka sulit menetapkan metode kerja. Studi menyatakan para penegak hukum berulang kali tidak mempunyai akses ke teknologi atau pelatihan yang memadai dalam menghadapi kejahatan AI, sehingga mereka rentan tertinggal oleh pelaku yang memanfaatkan teknologi canggih.¹⁷ Tanpa peningkatan kapasitas teknis dan pendidikan khusus (misalnya sertifikasi forensik digital), aparat sulit mengidentifikasi ciri *deepfake* maupun memahami jalur serangan siber yang digunakan pelaku. Upaya internasional seperti platform kolaborasi forensik atau bantuan teknis global belum optimal dijalankan.

Di luar ranah hukum dan teknis, faktor sosial budaya turut memperberat penanganan kasus *deepfake* pornografi. Masyarakat Indonesia umumnya masih rendah literasi *digital*, yaitu pemahaman bagaimana melindungi diri dan data di dunia maya. Indeks literasi digital Indonesia (2022) hanya 3,54 (skala 1–5) yang baru masuk kategori sedang.¹⁸ Artinya,

¹² Ibid

¹³ Mongkau, N. H., Bawole, H. Y. A., & Musa, A. (2025). Penegakkan Hukum Terhadap Penyalhgunaan Kecerdasan Buatan Dengan Cara Memanipulasi Wajah Seseorang Ke Dalam Gambar Atau Video Porno. *LEX ADMINISTRATUM*, 13(2).

¹⁴ Wahyudi, B. R. (2025). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI. *Innovative: Journal Of Social Science Research*, 5(1), 3436-3450.

¹⁵ Ibid

¹⁶ Gandrova, S., & Banke, R. (2023). Penerapan Hukum Positif Indonesia Terhadap Kasus Kejahatan Dunia Maya *Deepfake*. *Madani: Jurnal Ilmiah Multidisiplin*, 1(10), 21-35.

¹⁷ Wahyudi, B. R. (2025) Op.cit

¹⁸ Annur, C. M., (2023) Literasi Digital Indonesia Naik pada 2022, tapi Budaya Digital Turun <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/494c92f675bffc/literasi-digital-indonesia->

kesadaran akan risiko penyalahgunaan konten multimedia masih minim. Banyak orang tidak tahu bagaimana memverifikasi keaslian suatu video online, atau keberadaan undang-undang yang dapat melindungi jika mereka menjadi korban. Hal ini berpotensi membuat korban *deepfake* tidak segera menyadari telah menjadi target kejahatan, apalagi melapor ke otoritas hukum.

Kurangnya *awareness* hukum juga signifikan. Sebagian masyarakat awam belum terbiasa melaporkan kejahatan siber karena tidak paham mekanismenya. Di samping itu, masih marak kepercayaan salah bahwa “kalau dihapus, selesaikan sendiri”, sehingga korban enggan ke polisi. Padahal sebagaimana dikutip Komnas Perempuan, *deepfake* pornografi sejatinya merupakan salah satu bentuk kekerasan berbasis gender (KBGO) dan negara telah memberikan payung hukum (UU ITE, UU Pornografi). Meski begitu, korban sering tak sadar hak hukumnya.¹⁹

Stigma sosial terhadap korban pornografi menjadi penghalang utama. Banyak korban *deepfake*, khususnya perempuan, takut mengungkap kasus karena khawatir dicap negatif. Seperti dilaporkan, Warga negara yang banyak melakukan pemojokan terhadap para korban, Perempuan yang dijadikan objek dari kejahatan pornografi menggunakan *deepfake* banyak menerima perkataan negative serta pengucilan.²⁰ Kasus nyata terjadi di Bali baru baru ini, di mana puluhan mahasiswa perempuan menjadi korban *deepfake* pornografi. Para korban banyak memilih bungkam dan belum melapor kepada polisi karena khawatir dampak sosial dan tersebarnya konten lebih luas. Fakta ini menandakan bahwa stigma dan ketidaksiapan sosial menghambat pelaporan dan pemulihan korban.

Terakhir, kurangnya edukasi atau kampanye publik mengenai bahaya *deepfake* pornografi membuat penanggulangan hanya bergantung pada korban atau organisasi masyarakat. Pemerintah dan lembaga terkait belum optimal menyosialisasikan aturan dan mekanisme pelaporan yang jelas. Kondisi ini memperlebar kesenjangan antara perkembangan teknologi dan pemahaman publik. Secara keseluruhan, rendahnya literasi digital, minimnya kesadaran hukum, dan stigma berat terhadap korban mengakibatkan banyak kasus *deepfake* pornografi tidak terungkap secara tuntas – hal yang justru meningkatkan peluang pelaku luput dari jeratan hukum.

KESIMPULAN

Teknologi *deepfake* merupakan salah satu hasil perkembangan kecerdasan buatan yang mampu memanipulasi wajah, suara, atau gerak tubuh seseorang menjadi konten digital baru yang tampak realistis. Meskipun teknologi ini memiliki potensi untuk dimanfaatkan secara positif di berbagai sektor, dalam praktiknya justru lebih banyak digunakan untuk tujuan yang merugikan, termasuk membuat dan menyebarkan konten pornografi, menipu publik dengan informasi palsu, atau bahkan menjatuhkan reputasi seseorang secara sosial.

Kesimpulan dari pembahasan mengenai pemidanaan terhadap pelaku konten pornografi yang menggunakan teknologi *deepfake* menunjukkan bahwa kemajuan teknologi kecerdasan buatan, khususnya *deepfake*, telah membawa dampak signifikan terhadap dunia hukum, terutama dalam aspek perlindungan terhadap korban kejahatan berbasis digital. Teknologi *deepfake* memungkinkan seseorang untuk merekayasa konten visual, seperti merubah wajah pada video menggunakan wajah milik orang lain, dan dalam konteks pornografi, hal ini

[naik-pada-2022-tapi-budaya-digital-turun#:~:text=Menurut%20laporan%20tersebut%2C%20indeks%20literasi, sedang](#) Diakses pada 8 Juni 2025

¹⁹ Aprilia, R., (2024) Ancaman *Deepfake* Porn: Kekerasan Seksual Berbasis Digital dan Kesenjangan Regulasi di Indonesia <https://retizen.republika.co.id/posts/491063/ancaman-deepfake-#:~:text=Deepfake%20porn%20adalah%20salah%20satu,yang%20sering%20menjadi%20target%20utama> Diakses pada 8 Juni 2025

²⁰ Ibid

berujung pada bentuk eksploitasi digital yang merugikan korban secara personal, psikologis, dan sosial. Dalam konteks hukum pidana Indonesia, pelaku penyebaran konten pornografi *deepfake* sebenarnya dapat dijerat dengan berbagai regulasi yang sudah ada, seperti Undang-Undang Pornografi, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang Perlindungan Data Pribadi (UU PDP). Namun demikian, hingga saat ini, belum terdapat satu pun ketentuan hukum yang secara khusus mengatur atau menyebut teknologi *deepfake* secara eksplisit. Hal ini menimbulkan kekosongan hukum yang berimplikasi pada kesulitan dalam proses penegakan hukum, khususnya terkait pembuktian unsur-unsur tindak pidana serta identifikasi pelaku di ruang siber.

Dalam hal pidana, pelaku dapat dikenakan sanksi pidana jika dapat dibuktikan bahwa konten yang disebarluaskan termasuk ke dalam kategori pornografi sebagaimana diatur dalam UU Pornografi. Di sisi lain, jika penyebarannya dilakukan secara elektronik dan menimbulkan kerugian atau mencemarkan nama baik korban, maka UU ITE dapat digunakan sebagai dasar untuk menjerat pelaku. Namun penggunaan pasal-pasal ini masih terbatas pada pendekatan interpretatif, mengingat karakteristik *deepfake* belum tertuang secara khusus dalam ketentuan peraturan perundang-undangan. Penegakan hukum terhadap kasus *deepfake* pornografi di Indonesia masih dihadapkan pada berbagai tantangan. Selain kendala yuridis berupa belum adanya pengaturan yang tegas, aparat penegak hukum juga masih mengalami hambatan teknis dalam mengidentifikasi dan membuktikan konten *deepfake*. Keahlian dalam digital forensik masih sangat terbatas, sementara para pelaku kerap beroperasi secara anonim dan lintas negara, menjadikan proses pelacakan menjadi kompleks. Di sisi lain, korban kerap kali mengalami trauma, rasa malu, dan takut mengalami stigma sosial sehingga enggan untuk melaporkan kejadian yang dialaminya.

Melihat masih terbatasnya regulasi serta tantangan dalam penegakan hukum terhadap kejahatan berbasis *deepfake*, diperlukan langkah-langkah konkret yang dapat ditempuh oleh pembuat kebijakan, aparat penegak hukum, dan masyarakat secara luas. Pemerintah melalui lembaga legislatif sebaiknya segera merancang regulasi baru atau menyisipkan ketentuan khusus dalam undang-undang yang sudah ada untuk secara tegas mengatur penggunaan dan penyalahgunaan teknologi kecerdasan buatan, termasuk *deepfake*. Pengaturan tersebut perlu mencakup batasan etik, mekanisme perizinan, dan ancaman pidana bagi pelaku penyalahgunaan, serta mekanisme perlindungan dan pemulihan bagi korban.

Dengan demikian, diperlukan langkah-langkah serius dan sistematis dari pemerintah untuk membentuk kerangka hukum yang lebih adaptif terhadap perkembangan teknologi, termasuk dengan mempertimbangkan pembentukan undang-undang khusus yang mengatur penyalahgunaan teknologi *deepfake*. Hukum pidana tidak hanya dituntut untuk represif dalam penindakan, tetapi juga harus mampu bersifat preventif melalui pengaturan yang memberikan perlindungan secara menyeluruh terhadap hak-hak individu di era digital. Penanganan kejahatan *deepfake* pornografi bukan hanya sekadar masalah hukum, melainkan juga mencerminkan komitmen negara dalam menjaga martabat dan integritas setiap warga negara di tengah arus transformasi digital yang kian cepat.

REFERENSI

- Annur, C. M., (2023) Literasi Digital Indonesia Naik pada 2022, tapi Budaya Digital Turun <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/494c92f675bfffcc/literasi-digital-indonesia-naik-pada-2022-tapi-budaya-digital-turun#:~:text=Menurut%20laporan%20tersebut%2C%20indeks%20literasi,sedang>
Diakses pada 8 Juni 2025
- Aprilia, R., (2024) Ancaman *Deepfake* Porn: Kekerasan Seksual Berbasis Digital dan Kesenjangan Regulasi di Indonesia

- <https://retizen.republika.co.id/posts/491063/ancaman-deepfake-#:~:text=Deepfake%20porn%20adalah%20salah%20satu,yang%20sering%20menjadi%20target%20utama> Diakses pada 8 Juni 2025
- Arvitto R. (2024). Implikasi Hukum *Deepfake*: Telaah terhadap UU ITE dan UU PDP. 4.2 73-82
- Deeptrace (2019), “The State of *Deepfakes*: Landscape, Threats and Impact.” https://regmedia.co.uk/2019/10/08/deepfake_report.pdf Diakses pada 25 Mei 2025
- Fadhilah, a. D. Z., & Retnoningsih, s. (2024). Perancangan kampanye digital melawan disinformasi melalui artificial intelligence dan *Deepfake* di kalangan pra lansia usia 45-55 tahun. *Fad*, 3(02).
- Ferdinal, O., & Bakir, H. (2024). Legal Protection Efforts and Policies to Combat *Deepfake* Porn Crimes with Artificial Intelligence (AI) in Indonesia. *Journal of Multidisciplinary Sustainability Asean*, 1(6), 465-474.
- Gandrova, S., & Banke, R. (2023). Penerapan Hukum Positif Indonesia Terhadap Kasus Kejahatan Dunia Maya *Deepfake*. *Madani: Jurnal Ilmiah Multidisiplin*, 1(10), 21-35.
- Mongkau, N. H., Bawole, H. Y. A., & Musa, A. (2025). Penegakkan Hukum Terhadap Penyalhgunaan Kecerdasan Buatan Dengan Cara Memanipulasi Wajah Seseorang Ke Dalam Gambar Atau Video Porno. *LEX ADMINISTRATUM*, 13(2).
- Patikasari, T. *Pelindungan Hukum Bagi Korban Deepfake Pornografi (Studi Perbandingan Indonesia dan Korea Selatan)* (Bachelor's thesis, Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta).
- Situmeang, B. S., Dkk. (2024). Pengaruh *Artificial Intelligence* Terhadap Tingkat Kasus *Deepfake* Pada Selebritas di Twitter. *Device*, 14(1).
- Suseno S., (2012), *Yurisdiksi tindak pidana siber*, Bandung: Refika Aditama
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.
- UU No. 44/2008 tentang Pornografi
- Undang-Undang Nomor 22 tahun 2022 tentang Perlindungan Data Pribadi
- Wahyudi, B. R. (2025). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI. *Innovative: Journal Of Social Science Research*, 5(1), 3436-3450.