ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 26179-26188
Volume 7 Nomor 3 Tahun 2023

Analisis Hukum terhadap Upaya Pencegahan Kasus *Deepfake Porn* dan Pendidikan Kesadaran Publik di Lingkungan Digital

Andhika Nugraha Utama[1], Prama Tusta Kesuma[2], Rio Maulana Hidayat[3]

[1,2,3] Fakultas Hukum Universitas Pakuan

e-mail : andhikanugrahautama@gmail.com [1], ramatusta08@gmail.com [2], riomaulanax@gmail.com [3]

Abstrak

Penelitian ini membahas pencegahan *deepfake porn* dan peran penting pendidikan kesadaran publik di ranah digital. Penekanan diberikan pada peran hukum dan teknologi dalam mengatasi deepfake. Melalui metode yuridis normatif, penelitian mengidentifikasi masalah hukum *deepfake* yang memerlukan reformasi hukum spesifik. Identifikasi deepfake yang canggih adalah alat utama dalam menghapus konten merugikan. Di Indonesia, belum ada undang-undang yang mengatur penggunaan AI, sehingga perlindungan hukum belum memadai. Penelitian ini menyarankan undang-undang AI yang khusus. Pendidikan kesadaran publik tentang *deepfake* sangat penting, tetapi regulasi yang mewajibkan penyedia platform digital untuk menyediakan pendidikan perlu diimplementasikan. Pengembangan teknologi identifikasi *deepfake* perlu diinvestasikan, dan kolaborasi internasional serta evaluasi program pendidikan kesadaran esensial dalam pencegahan *deepfake porn*. Kesimpulan penelitian adalah pencegahan *deepfake porn* memerlukan kerjasama antara hukum, teknologi, dan pendidikan kesadaran untuk melindungi masyarakat dan mencegah penyebaran konten berbahaya.

Kata Kunci : *Deepfake Porn, Regulasi Hukum, Teknologi.*

Abstract

This research discusses the prevention of deepfake porn and the important role of public awareness education in the digital realm. Emphasis is placed on the role of law and technology in addressing deepfakes. Through normative juridical methods, the research identifies deepfake legal issues that require specific legal reforms. Sophisticated deepfake identification is a key tool in removing harmful content. In Indonesia, there is no law regulating the use of AI, so legal protection is inadequate. This research suggests a specialized AI law. Public awareness education on deepfakes is essential, but regulations requiring digital platform providers to provide education need to be implemented. Development of deepfake identification technology needs to be invested in, and international collaboration and evaluation of awareness education programs are essential in the prevention of deepfake porn. It is concluded that the prevention of deepfake porn requires cooperation between law, technology, and awareness education to protect the public and prevent the spread of harmful content.

Keywords : *Deepfake Porn, Legal Regulations, Technology*

PENDAHULUAN

Dalam era yang semakin maju secara digital, kemajuan teknologi informasi telah memberikan dampak positif yang sangat besar pada berbagai sektor kehidupan. Namun, seiring dengan perkembangan teknologi tersebut, muncul pula tantangan baru dalam bentuk penyalahgunaan teknologi yang berpotensi merugikan individu maupun masyarakat secara keseluruhan. Salah satu peristiwa yang mencuat dalam beberapa tahun terakhir adalah fenomena "*Deepfake Porn*."

Salah satu karya *Artificial Intelligence* (AI) yang menjadi sorotan adalah *deepfake*. *Deepfake* merujuk pada penggabungan teknologi *deep learning* dengan tujuan menciptakan konten palsu. *Deep learning*, pada dasarnya, adalah teknik yang digunakan untuk melatih AI agar dapat mengeksekusi suatu tugas tertentu. *Deepfake* adalah Istilah yang digunakan untuk algoritma tersebut adalah teknik pemrosesan video yang memungkinkan pengguna untuk mengganti wajah satu aktor dengan wajah aktor lain dalam video dengan tingkat keaslian gambar yang tinggi yakni meniru objek visual yang nyata. Selain dalam bentuk video, teknologi *deepfake* juga dapat digunakan untuk merekayasa gambar. *Deepfake Porn* yaitu penggunaan teknologi untuk menciptakan video pornografi palsu dengan menggantikan wajah individu yang sebenarnya dengan wajah orang lain. Permasalahan ini memiliki potensi merusak citra individu, privasi, dan kesejahteraan psikologis pihak yang terlibat.

Pada tahun 2017, istilah "*deepfake*" mulai mendapatkan perhatian luas berkat seorang pengguna Reddit yang memanfaatkan *Generative Adversarial Networks* (GAN), Sebuah prosedur pembelajaran mesin, serta TensorFlow, sebuah perangkat lunak yang dibuat oleh Google untuk memperdalam pemahaman dan pembelajaran mesin. Kombinasi GAN dan TensorFlow memungkinkan pembuatan video palsu atau *deepfake* yang mencampurkan tubuh atau wajah tokoh publik atau selebriti ke dalam konten porno yang sudah ada. Semakin banyak sampel gambar wajah dan rekaman suara yang tersedia dari subjek sumber, semakin realistis dan autentik kontennya. Oleh karena itu, menentukan apakah konten dibuat dengan teknologi *deepfak*e menjadi semakin sulit karena tingkat realisme yang tinggi. Kehadiran teknologi ini telah menimbulkan kekhawatiran yang signifikan terkait dengan potensi dan dampak negatif dari *deepfake*, yang memiliki kemampuan untuk mengelabui penglihatan manusia dan mengakibatkan permasalahan serius terkait pemalsuan dan penyebaran konten pornografi palsu yang melibatkan figur publik terkenal.

Setelah munculnya aplikasi yang dikenal dengan nama *FakeApp* pada bulan Januari 2018, permasalahan yang berkaitan dengan teknologi *deepfake* menjadi semakin serius. *FakeApp* merupakan sebuah aplikasi yang dapat diakses oleh siapa saja, yang memungkinkan pengguna untuk menciptakan gambar dan klip video yang tidak asli. Ketakutan akan potensi penyalahgunaan dan dampak negatif dari penggunaan aplikasi ini telah meningkat seiring dengan kemudahan penggunaannya. Oleh karena itu, pengguna perlu selalu berpikir kritis dan bijak ketika menggunakan teknologi seperti kecerdasan buatan, untuk menghindari timbulnya gangguan dalam masyarakat atau kerusakan pada hubungan antarindividu.

Penyalahgunaan teknologi *deepfake* ini memunculkan tantangan serius dalam konteks hukum dan etika. Berdasarkan jenis kejahatan tersebut merujuk pada ketentuan dalam UU ITE dan perubahannya, UU PDP, UU Pornografi, atau UU 1/2023 tentang KUHP baru. Hal ini menimbulkan pertanyaan tentang batasan-batasan hukum yang ada dalam penanganan kasus-kasus *Deepfake* Porn, serta bagaimana masyarakat dan individu dapat melindungi diri dari potensi penyalahgunaan teknologi ini. Oleh karena itu, studi ini bertujuan untuk melakukan analisis terhadap kerangka hukum yang terkait dengan upaya pencegahan kasus *Deepfake Porn*, sekaligus merumuskan pendekatan pendidikan kesadaran masyarakat dalam lingkungan digital sebagai alternatif solusi untuk mengatasi permasalahan tersebut.

Dalam menjawab tantangan yang telah disebutkan di atas, penelitian ini akan mengkaji berbagai aspek hukum yang terkait dengan *Deepfake Porn*, termasuk peranan hukum dalam melindungi privasi individu, hak cipta, dan keamanan siber. Lebih dari itu, penelitian ini juga akan menggali potensi pendidikan kesadaran masyarakat sebagai upaya pencegahan dengan meningkatkan pemahaman masyarakat tentang risiko *Deepfake* dan cara-cara melindungi diri dari kemungkinan penyalahgunaan teknologi ini.

Rencana pemecahan masalah mencakup analisis mendalam terhadap peraturan-peraturan yang berlaku, baik di tingkat nasional maupun internasional, serta identifikasi potensi reformasi hukum yang mungkin diperlukan untuk mengatasi dinamika perkembangan teknologi ini. Selain itu, penelitian ini akan merumuskan saran-saran praktis untuk pendidikan kesadaran masyarakat yang efektif, termasuk metode pelatihan dan penyebaran informasi yang dapat meningkatkan pemahaman masyarakat tentang *Deepfake Porn*.

Untuk lebih mendalami pemecahan masalah terkait *Deepfake Porn*, perlu juga mempertimbangkan kerjasama internasional dalam hal ini. Seiring dengan sifat global internet, *Deepfake Porn* dapat melintasi batas negara dengan mudah, membuatnya menjadi tantangan yang bersifat lintas batas. Oleh karena itu, kerjasama antarnegara dalam pertukaran informasi dan koordinasi tindakan hukum sangat penting. Penelitian ini akan melibatkan analisis kerangka kerjasama internasional dalam menangani masalah teknologi seperti ini, termasuk perjanjian bilateral dan multilateral yang ada.

Penting juga untuk menyadari bahwa teknologi yang digunakan untuk *Deepfake Porn* dapat digunakan untuk tujuan lain yang tidak etis atau ilegal. Oleh karena itu, dalam pemecahan masalah ini, harus dipertimbangkan dampak yang lebih luas dari teknologi ini pada masyarakat dan masyarakat global. Ini mungkin mencakup pengembangan etika teknologi yang lebih ketat, pemantauan teknologi yang lebih cermat, dan regulasi yang lebih baik dalam pengembangan dan penggunaan algoritma *Deepfake Porn*.

Selain itu, penyadaran dan pendidikan tidak hanya diperlukan untuk masyarakat umum, tetapi juga bagi lembaga pendidikan, organisasi, dan perusahaan yang mungkin menjadi sasaran potensial penyalahgunaan teknologi *Deepfake*. Membekali mereka dengan pemahaman tentang bagaimana melindungi data pribadi dan citra diri adalah langkah penting dalam memitigasi risiko ini.

Terakhir, penting untuk menciptakan mekanisme pelaporan yang aman dan efisien bagi individu yang menjadi korban *Deepfake Porn*. Mereka perlu tahu bahwa mereka memiliki dukungan hukum dan mekanisme untuk menghilangkan konten yang melanggar hak privasi mereka. Penelitian ini juga akan mempertimbangkan cara-cara untuk meningkatkan akses individu yang terkena dampak ke bantuan hukum dan dukungan psikologis.

Dengan menjalani pendekatan komprehensif yang mencakup hukum, pendidikan kesadaran masyarakat, kerjasama internasional, etika teknologi, dan mekanisme pelaporan, kita dapat bergerak maju dalam mengatasi tantangan serius yang disajikan oleh *Deepfake Porn.* Ini adalah langkah yang penting dalam menjaga integritas, privasi, dan kesejahteraan psikologis individu di era digital yang terus berkembang.

METODE

Metode penelitian yang dapat digunakan untuk menganalisis upaya pencegahan *deepfake* pornografi dan pendidikan kesadaran publik di lingkungan digital adalah metode penelitian yuridis normatif. Langkah-langkah dalam metode ini meliputi identifikasi masalah hukum yang akan diteliti, pengumpulan data melalui penelusuran peraturan dan literatur terkait dengan masalah yang diteliti, analisis data dengan menggunakan pendekatan normatif yang berfokus pada hukum dan peraturan yang berlaku, dan penarikan kesimpulan berdasarkan analisis data tersebut. Dalam hal ini, peneliti akan menganalisis peraturan dan hukum yang berlaku terkait dengan *deepfake* pornografi dan pendidikan kesadaran publik di lingkungan digital untuk menghasilkan kesimpulan terkait dengan upaya pencegahan dan penanggulangan masalah tersebut dalam kerangka hukum yang berlaku. Pengumpulan data dapat dilakukan melalui penelusuran peraturan dan literatur, baik di perpustakaan maupun sumber online seperti jurnal dan situs web pemerintah.

HASIL DAN PEMBAHASAN

Metode penelitian ini menghasilkan pemahaman yang lebih dalam tentang upaya pencegahan kasus *deepfake porn* dan pentingnya pendidikan kesadaran publik di lingkungan digital. Dengan demikian, penelitian ini dapat menjadi dasar bagi pengembangan kebijakan yang lebih efektif dalam melindungi individu dan masyarakat dari risiko *deepfake porn* serta meningkatkan kesadaran publik tentang masalah ini. Hasil utama dari analisis ini adalah bahwa hukum dan teknologi memiliki peran kunci dalam upaya pencegahan kasus *deepfake porn*. Peraturan hukum yang kuat dan efektif adalah fondasi yang diperlukan untuk memerangi praktik *deepfake*, sementara teknologi identifikasi *deepfake* yang canggih membantu dalam mengidentifikasi dan menghapus konten yang merugikan.

Perubahan dalam Sistem Hukum Untuk Mengatur Situasi Di Mana Terjadi Penyebaran Konten *Deepfake Porn*.

Kemampuan untuk melakukan pemikiran rasional dan mengambil langkah-langkah yang paling efisien adalah salah satu karakteristik utama dari kecerdasan buatan (AI). Penelitian yang berkaitan dengan kemampuan komputer dalam melaksanakan pekerjaan yang dapat dilakukan oleh manusia saat ini semakin berkembang dengan baik. Bidang-bidang seperti penalaran, pembelajaran, dan berbagai domain lainnya adalah area di mana kecerdasan buatan akan diterapkan. Kecerdasan buatan (AI) sebenarnya adalah istilah yang keliru karena yang dimaksud bukanlah kecerdasan sama sekali, saat ketika McCarthy menciptakan suatu istilah "kecerdasan buatan", yang dia pikirkan adalah pembelajaran mesin, algoritma yang membangun model matematika dari sekumpulan data untuk memungkinkan prosesor membuat prediksi tidaklah seperti penalaran manusia, meskipun pada saat ini mesin tidak dapat berpikir dan membuat pilihan yang rasional dan otonom. Ketika kecerdasan buatan melakukan otomatisasi dalam pengolahan data, hal ini dapat dianggap sebagai sebuah "Entitas Elektronik" sesuai dengan peraturan di Indonesia. Pasal 1 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menggambarkan agen elektronik sebagai :

"*Informasi Elektronik adalah satu atau sekelompok data elektronik, termasuk namun tidak terbatas pada teks, suara, gambar, peta, rancangan, foto, pertukaran data elektronik (EDI), surat elektronik (email), telegram, teleks, telekopi, atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah dan memiliki makna atau dapat dimengerti oleh individu yang mampu memahaminya.*.".

Meskipun undang-undang Informasi dan Transaksi Elektronik (ITE) mengelola penggunaan teknologi kecerdasan buatan, masih ada tantangan yang sulit diatasi. Salah satu contoh masalah adalah penyalahgunaan *deepfake*, Di tahun 2019, *Deeptrace* melakukan sebuah penelitian dan menemukan bahwa 96% dari video *deepfake* berisikan materi berbau pornografi. Hal ini berpotensi mengakibatkan dampak finansial dan psikologis yang merugikan bagi individu yang menjadi korban. Hal ini semakin diperparah oleh kesulitan yang dihadapi masyarakat dalam membedakan gambar atau video yang telah dimanipulasi karena kemajuan terus-menerus dalam teknologi kecerdasan buatan.

Karena belum ada undang-undang khusus yang mengatur *deepfake*, Pelaku kejahatan semacam ini sering kali terhindar dari sanksi hukum yang sesuai. Saat ini, hanya undang-undang yang berkaitan dengan informasi elektronik, etika, pornografi, dan pencemaran nama baik yang bisa diterapkan untuk mengatasi pelanggaran-pelanggaran ini. Namun, efektivitas sanksi yang ada masih diragukan karena tidak ada kerangka hukum yang khusus dan tegas untuk melindungi masyarakat dari ancaman *deepfake*.

Karena perbedaan mendasar antara teknologi dan manusia, ada argumen yang menyatakan bahwa teknologi tidak terikat oleh batasan moral. Individu memiliki kapabilitas untuk mengkomprehensif, memproses informasi, dan mengambil tindakan yang selaras dengan prinsip-prinsip moral yang dianut dalam lingkungan sosial. Ini adalah perbedaan signifikan yang memisahkan manusia dari teknologi. Sebelum membuat keputusan, manusia memiliki kemampuan untuk mempertimbangkan aspek hukum dan dampak moral dari informasi yang mereka terima.

Sebaliknya, meskipun kecerdasan buatan (AI) memiliki kemampuan yang sangat kuat memproses data dan mengenali pola yang kompleks, AI hanya dapat beroperasi berdasarkan instruksi yang dibuat oleh orang. Dalam hal ini tentu terdapat risiko hilangnya informasi yang berguna dan bermanfaat sebagai konsekuensi dari perantara penyedia layanan Internet yang menerapkan filter Al pada rentang informasi yang terlalu sempit untuk menghindari penalti. Oleh karena itu, kecerdasan buatan tidak memiliki pemahaman inheren tentang nilai-nilai moral manusia, sehingga tidak mampu menetapkan apakah informasi yang diproses sesuai dengan standar, undang-undang, atau etika. Akibatnya, orang-orang, termasuk pengembang AI, bertanggung jawab atas penggunaan AI secara etis, hukum, dan moral.

Hingga saat ini, di Indonesia, belum ada undang-undang yang secara khusus dan rinci mengatur penggunaan kecerdasan buatan (AI). Peraturan yang telah ada saat ini mengatasi AI sebagai agen elektronik, yakni perangkat elektronik yang dapat menjalankan tugas-tugas

otomatis terkait informasi elektronik. Akan tetapi, peraturan tersebut tidak sepenuhnya menyentuh situasi yang lebih dalam terkait dengan etika, privasi, dan konsekuensi sosial dari penggunaan AI. Kekurangan kerangka dasar hukum yang jelas dan spesifik untuk AI bisa menimbulkan keraguan seputar tanggung jawab, etika, dan konsekuensi sosial dari teknologi AI.

Pasal 21 dari Undang-undang Informasi dan Transaksi Elektronik memberikan definisi untuk agen elektronik sebagai sebuah entitas. Namun, AI tidak memiliki regulasi khusus karena sifatnya yang *open-source*. Ini berbeda dengan platform digital lainnya, seperti situs *Platform e-commerce* seperti Bukalapak dan Tokopedia memiliki regulasi yang lebih ketat dalam mengatur sistem elektronik mereka. Hal ini menjadi unik karena AI *open-source* tidak dikendalikan oleh perusahaan atau individu yang mengelola sistem elektronik. Oleh karena itu, peraturan yang ada saat ini belum mencakup AI secara menyeluruh.

Menurut teori Profesor Mochtar Kusumaatmadja, hukum seharusnya "berada di depan" dalam menciptakan lingkungan teknologi-sosial yang sehat. Regulasi kemudian akan membimbing para pemangku kepentingan. Salah satu peran penting undang-undang adalah menetapkan standar mengenai bagaimana Kemampuan AI untuk menjadi subjek hukum yang memiliki tanggung jawab atas tindakannya dapat meningkatkan efektivitas penegakan hukum dalam situasi pelanggaran. Oleh karena itu, peran badan pengatur sangat penting dalam menjaga hak-hak masyarakat dan menciptakan kondisi yang mendukung kemajuan AI.

Salah satu hal yang sangat penting adalah adanya undang-undang khusus yang mengatur AI. Hal ini diperlukan bukan hanya untuk melindungi korban *deepfake* pornografi, tetapi juga karena teknologi yang semakin maju memungkinkan berbagai bentuk kejahatan lainnya untuk berkembang tanpa batas. Dalam kemajuan teknologi ini membuat banyak tren-tren yang menggunakan teknologi, contohnya *deepfake* ini, memang benar bentuknya tidak hanya pornografi, ada juga beberapa pemimpin politik yang menjadi korban atas *deepfake* ini, sehingga dapat menimbulkan kekhawatiran dan kehebohan serta ketakutan umum atas adanya konten video yang seakan akan itu adalah para pemimpin politik tersebut. Tentu hal ini berisiko memperdalam sinisme serta melemahkan kepercayaan publik terhadap komunikasi politik. Pakar hukum Bobby Chesney dan Danielle Citron (2019) mengidentifikasi masalah yang mereka sebut sebagai *Liar's Dividend* (Pembohong Dividen), yaitu kesadaran masyarakat akan kemungkinan *deepfake* yang memudahkan konten nyata untuk dianggap palsu. Ardi, yang merupakan Ketua Indonesia Cyber Security Forum (ICSF), telah menegaskan bahwa forensik digital juga memerlukan teknologi canggih yang setara untuk mengidentifikasi keaslian gambar atau video yang dikirim melalui email.

Instrumen Regulasi Sebagai Penindak Para Pelaku dari Kasus *Deepfake Porn* dan Efektivitasnya dari Hukum yang Ada

Saat ini, di Indonesia belum ada peraturan yang komprehensif dan khusus yang mengatur penggunaan teknologi AI dalam pembuatan *deepfake* berisi konten pornografi. Hal ini dikarenakan penyebaran foto atau video melalui internet dianggap sebagai tindakan kriminal dalam ranah dunia maya atau *cybercrime*, dan induknya adalah *cyberspace*. *Cyberspace* dipandang sebagai sebuah dunia komunikasi yang berbasis komputer, *cyberspace* dianggap sebagai sebuah realitas baru dalam kehidupan manusia yang dalam bahasa sehari-hari dikenal dengan internet. Tindakan *deepfake* tergolong dalam suatu bentuk kejahatan siber. Karena sangat jelas bahwa *deepfake* merupakan suatu bentuk *illegal contents,* yaitu konten yang dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Di Indonesia, ada beberapa undang-undang yang mengatur pornografi, seperti aturan yang dapat diterapkan terkait informasi elektronik, etika, pornografi, dan pencemaran nama baik. Oleh karena itu, Penyebaran materi deepfake yang berisikan konten pornografi, pelecehan, atau pencemaran nama baik akan dikenai sanksi sesuai dengan UU ITE, yaitu undang-undang yang berfokus pada regulasi transaksi elektronik. Pasal 27 ayat (1) UU ITE mencakup situasi di mana terdapat penyebaran informasi pornografi melalui media elektronik. Pasal tersebut menjelaskan bahwa "mendistribusikan" mencakup tindakan mengirim dan menyebarkan Informasi Elektronik serta Dokumen Elektronik kepada berbagai pihak atau

publik melalui Sistem Elektronik. "Mentransmisikan" merujuk pada pengiriman Informasi Elektronik dan Dokumen Elektronik kepada pihak lain melalui Sistem Elektronik. Sementara "membuat dapat diakses" mencakup segala tindakan selain mendistribusikan dan mentransmisikan melalui Sistem Elektronik yang membuat Informasi Elektronik dan Dokumen Elektronik dapat diketahui oleh pihak lain atau masyarakat umum.

Selain itu, peraturan hukum melarang modifikasi atau produksi data elektronik untuk tampak otentik. Tindakan seseorang yang mengubah gambar, misalnya, mengubah citra seseorang yang berpakaian menjadi telanjang seakan-akan itu merupakan gambaran yang sebenarnya, melanggar undang-undang. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Pelaku akan menghadapi hukuman penjara setidaknya dua belas tahun dan denda setidaknya dua belas miliar rupiah. "Setiap orang yang memenuhi syarat-syarat yang disebutkan dalam pasal 35 akan dipidana dengan pidana penjara tidak lebih dari 12 (dua belas) tahun dan/atau denda tidak lebih dari 12.000.000.000,00 (dua belas miliar rupiah)." Pernyataan ini sesuai dengan isi Pasal 51 UU Nomor 11 Tahun 2008.

Namun, penggunaan teknologi kecerdasan buatan dalam pornografi tidak diatur oleh UU ITE. Kompleksitas teknologi bisa membuat penegak hukum kesulitan dalam mengidentifikasi pelaku karena mereka dapat menyembunyikan jejak digital mereka. Selain itu, dalam konteks *deepfake*, Isu penerapan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memerlukan pertimbangan yang seimbang antara menjaga privasi dan kebebasan berekspresi. Penting untuk melindungi korban tanpa mengorbankan hak privasi dan kebebasan berekspresi individu secara keseluruhan.

Mengingat *deepfake* pornografi merupakan pelanggaran hukum pornografi, secara logis, hal ini juga terkait dengan KUHP, yang mengatur pelanggaran pornografi di Indonesia. Pornografi termasuk dalam klasifikasi tindakan ilegal yang melanggar etika moral sesuai dengan Bagian Keempat Belas mengenai Tindakan Melanggar Kesusilaan dalam KUHP, yang meliputi Pasal 281 hingga 283 KUHP.

Dengan perkembangan teknologi informasi, definisi pornografi dalam masyarakat telah berubah, dan perubahan ini seharusnya mempengaruhi cara kita memahami unsur-unsur pornografi. Konsep "umum" dalam situasi ini perlu diartikan dengan lebih inklusif, mengingat perkembangan teknologi informasi saat ini. Layar komputer yang digunakan oleh perusahaan rental, kantor, atau individu tidak dapat dianggap sebagai sesuatu yang dapat diakses oleh semua orang sesuai dengan Pasal 282 KUHP.

Selain itu, Pasal 282 KUHP tidak secara eksplisit membatasi kesusilaan. Dalam pernyataannya, ia Mengatakan bahwa penilaian tentang perilaku cabul atau norma kesopanan seharusnya bergantung pada pandangan umum dan adat istiadat lokal. Ini menunjukkan bahwa tidak ada batasan yang pasti terkait dengan pornografi atau tindakan cabul itu sendiri; yang mengikat hanyalah konteks sosial dan perkembangan yang telah terjadi. Sebagai hasilnya, batasan yang tidak jelas dalam KUHP mengenai pornografi bisa diinterpretasikan dengan berbagai cara.

Ini bukan hanya masalah teoritis, tetapi juga memiliki dampak dalam kehidupan nyata. Penegak hukum tidak dapat bertindak tanpa dukungan dari akademisi, praktisi hukum, dan ahli teknologi informasi. Sangat penting untuk membatasi perbuatan yang dianggap melanggar kesusilaan, karena penegakan hukum pidana harus berlangsung secara objektif. Pasal-pasal hukum pidana tidak boleh diinterpretasikan dengan cara yang berbeda, karena tujuan penegakan hukum pidana harus tetap konsisten.

Pelaku kejahatan semacam itu dianggap memiliki ancaman pidana yang kurang signifikan, terutama dalam hal pidana denda. Keseluruhan KUHP memiliki kelemahan karena dibuat pada masa kolonial Belanda. Meskipun jumlah denda pidana telah mengalami perubahan,Perubahan ini sudah lama berlalu. Perubahan signifikan terkait besaran denda dalam KUHP terjadi melalui Peraturan Pemerintah Pengganti Undang-Undang (Perpu) Nomor 18 Tahun 1960. Peraturan ini mengatur peningkatan jumlah sanksi denda dalam KUHP serta

hukuman lainnya sebelum tanggal 17 Agustus 1945. Nilai denda ditetapkan dalam rupiah dan ditingkatkan lima belas kali melalui perubahan ini. Akibatnya, denda yang pada saat itu sangat kecil, berkisar antara Rp225 hingga Rp75.000, menjadi sangat kecil jika dibandingkan dengan nilai saat ini.

Dalam konteks penggabungan materi porno menggunakan teknologi *deepfake*, pengiriman informasi pornografi dari satu tempat ke tempat lain melalui metode kecerdasan buatan juga dapat diilustrasikan dengan cara serupa. "Telekomunikasi adalah tindakan mengirim, menerima, atau mentransmisikan data dalam bentuk apapun, seperti simbol, pesan, tanda, tulisan, gambar, suara, atau gelombang suara melalui sarana berbasis kabel, sistem optik, radio, atau elektromagnetik lainnya," sesuai dengan definisi yang tercantum dalam Pasal 1 ayat 1 dari Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Dalam konteks ini, teknologi seperti kecerdasan buatan dapat dianggap sebagai alat komunikasi karena mereka mampu mengirim dan menerima informasi melalui sistem elektromagnetik dalam berbagai format, seperti gambar, suara, dan video. Penggunaan internet yang mengganggu ketertiban umum atau privasi dapat menghasilkan seseorang menerima konsekuensi hukum. Meskipun demikian, Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi tidak mencakup pertukaran informasi elektronik melalui teknologi kecerdasan buatan. Aspek-aspek keamanan dalam pertukaran pesan melalui kecerdasan buatan juga tidak diatur dalam peraturan tersebut. Oleh karena itu, Indonesia memerlukan undang-undang khusus yang mengatur telekomunikasi melalui teknologi AI. Undang-undang ini akan mengatur penggunaan teknologi kecerdasan buatan dengan bijaksana, terutama dalam situasi gangguan besar-besaran.

Pentingnya Penting sekali untuk memastikan penggunaan teknologi AI yang bertanggung jawab dan etis dengan menggunakan sistem pemantauan dan alat deteksi deepfake yang sangat canggih. Selain itu, regulasi dan norma etika juga harus diperhatikan dalam pengembangan AI untuk memastikan penggunaannya yang adil, aman, dan menghormati privasi. Selain membuat peraturan, pendidikan kepada pengguna tentang AI sangat penting agar mereka dapat memahami dampak dan risiko teknologi ini. Hal ini akan membantu masyarakat menggunakan teknologi kecerdasan buatan dengan lebih bijaksana dan bertanggung jawab, dan sekaligus mencegah masalah hukum yang disebutkan sebelumnya.

Korban pornografi palsu harus mendapatkan perlindungan yang sesuai, termasuk alat yang kuat untuk melaporkan dan mengatasi akibat yang mereka alami, seperti pemalsuan foto atau video yang merusak reputasi mereka. Meskipun teknologi untuk mengidentifikasi *deepfake* terus berkembang, masih ada tantangan dalam mengidentifikasinya dengan cepat dan akurat. Oleh karena itu, diperlukan investasi dalam penelitian dan pengembangan teknologi yang lebih canggih untuk melawan ancaman *deepfake*.

Pentingnya Kesadaran Publik dan Mekanisme Penegakan Hukum Lintas Negara Dapat Diperkuat dalam Penegakan Hukum Serta Penuntutan Pelaku *Deepfake*

Kesadaran publik dan mekanisme penegakan hukum lintas negara sangat penting untuk penegakan hukum dan penuntutan pelaku *deepfake* di era digital. *Deepfake*, yaitu manipulasi citra dan video untuk membuat konten palsu, merupakan ancaman besar bagi dunia online. Kesadaran publik sangat penting sebagai langkah awal untuk memerangi fenomena ini. Dengan pemahaman yang lebih baik tentang *deepfake*, orang dapat menjadi lebih waspada terhadap ancaman yang mungkin, menemukan konten palsu, melaporkan pelanggaran, dan membantu korban.

Meningkatkan kesadaran publik di dunia digital juga merupakan langkah proaktif yang harus ditingkatkan. Masyarakat perlu dididik tentang bahaya pornografi *deepfake* dan cara mengidentifikasi konten yang telah dimanipulasi. Saat ini, belum ada peraturan yang mengharuskan penyedia platform digital untuk menyediakan pendidikan kesadaran publik. Oleh karena itu, peraturan yang lebih ketat diperlukan untuk memastikan kontribusi semua penyedia platform dalam pendidikan kesadaran ini.

Pendidikan terkait *deepfake* yang komprehensif juga diperlukan untuk meningkatkan kesadaran publik. Kampanye pendidikan harus mencakup informasi yang mudah dipahami masyarakat umum, menjelaskan bagaimana *deepfake* bekerja, dan memberikan contoh kasus terkenal yang melibatkan *deepfake*. Sekolah dan institusi pendidikan juga harus memainkan peran penting dalam mendidik siswa tentang cara membedakan konten palsu dan risiko *deepfake*. Media dan platform online dapat berperan dalam menyebarkan informasi ini secara luas dan memberi pengguna panduan praktis tentang cara melindungi diri.

Namun, untuk mengidentifikasi, mengejar, dan menuntut pelaku deepfake, mekanisme penegakan hukum lintas negara diperlukan. Mekanisme ini membantu dalam mengidentifikasi pelaku yang mungkin berada di luar yurisdiksi negara tempat korban berada, mengumpulkan bukti terkait deepfake, mengejar penuntutan pelaku di berbagai yurisdiksi, dan menciptakan kerangka hukum yang seragam.

Kemitraan antar negara juga penting dalam upaya pencegahan dan penegakan hukum terhadap pornografi *deepfake*, mengingat pelaku seringkali beroperasi di berbagai negara. Perjanjian ekstradisi yang efektif dan kerangka hukum yang kokoh diperlukan dalam hal ini. Evaluasi berkala tentang program pendidikan kesadaran publik, peraturan hukum, dan teknologi juga penting untuk memastikan efektivitas langkah-langkah yang diambil. Dengan pendekatan yang komprehensif dan berkelanjutan, kita dapat melindungi masyarakat dari bahaya pornografi *deepfake* dan mencegah penyebaran konten yang merugikan.

Kemudian, untuk meningkatkan mekanisme penegakan hukum lintas negara, negara-negara harus bekerja sama lebih aktif dan berbagi informasi tentang *deepfake*. Ini dapat dicapai melalui perjanjian yang dibuat antara dua negara dan antara tiga negara, serta perjanjian yang dibuat oleh lebih dari satu negara, yang menetapkan kerangka kerja kerja sama untuk memerangi deepfake. Pengembangan tim khusus yang bekerja secara lintas negara untuk menyelidiki kasus *deepfake* yang melibatkan pelaku di berbagai yurisdiksi adalah bagian dari upaya ini.

Dalam upaya ini, peran penyedia layanan digital, seperti platform media sosial dan situs web berbagi video, juga menjadi perhatian penting. Mereka harus memiliki kebijakan yang ketat terkait konten palsu dan *deepfake*, dan sistem yang efektif untuk melaporkan pengguna yang menemukannya. Untuk mengurangi efek *deepfake*, penyedia layanan dan pihak berwenang harus bekerja sama untuk menanganinya dan mengidentifikasi pelakunya.

Selain itu, transparansi platform dalam melacak dan menangani deepfake harus ditingkatkan. Ini termasuk fungsi yang dilakukan platform untuk mengidentifikasi, menghapus, dan melaporkan konten *deepfake* kepada pihak berwenang. Untuk mengurangi penyebaran deepfake di platform tersebut, sistem pemantauan yang lebih efektif harus digunakan. Terakhir, kolaborasi antar negara tidak hanya berkonsentrasi pada penegakan hukum, tetapi juga untuk membangun perjanjian internasional yang lebih kuat dan terbuka yang mengatur penanganan *deepfake*. Perjanjian ini dapat mencakup standar etika untuk penggunaan teknologi *deepfake*, kerangka hukum yang seragam, dan prosedur penyelidikan yang konsisten.

Meskipun penting, meningkatkan kesadaran publik dan mekanisme penegakan hukum lintas negara juga melibatkan sejumlah tantangan, seperti keterbatasan hukum saat ini, kompleksitas teknologi *deepfake*, kerja sama lintas negara yang rumit, dan pengawasan platform digital. Upaya yang dapat dilakukan untuk mengatasi tantangan ini meliputi kampanye pendidikan publik yang lebih luas, pengembangan hukum yang lebih kuat, dan peningkatan kerja sama lintas negara dalam penegakan hukum. Dengan langkah-langkah ini, negara-negara dapat bekerja sama secara internasional untuk memerangi *deepfake* dan masyarakat dapat menjadi lebih siap dan terlindungi dari ancaman ini.

Dengan kesadaran publik yang meningkat, mekanisme penegakan hukum yang diperkuat, dan kerja sama lintas negara yang lebih erat, upaya untuk mengatasi deepfake dan melindungi masyarakat dari dampak negatifnya dapat menjadi lebih efektif. Kesadaran publik yang luas akan membantu mencegah dan mengidentifikasi *deepfake*, sementara kerja sama lintas negara akan memungkinkan penegakan hukum yang lebih baik dan penuntutan yang

lebih kuat terhadap mereka yang melakukannya. Dengan langkah-langkah ini, kita dapat dengan lebih efektif menangani ancaman deepfake di era digital yang semakin kompleks ini.

SIMPULAN

Peraturan yang ketat dan efektif harus menjadi dasar penegakan hukum terhadap pelaku *deepfake*. Teknik identifikasi *deepfake* yang terus berkembang menjadi sarana penting untuk menemukan konten yang telah dimanipulasi. Sangat penting bagi upaya ini untuk melindungi korban, yang mencakup akses ke layanan hukum dan partisipasi masyarakat dalam melaporkan konten mencurigakan. Kolaborasi antar negara juga penting karena pelaku *deepfake porn* sering berasal dari berbagai negara. Pendidikan publik tentang keadaan digital dan evaluasi terus-menerus keberhasilan tindakan pencegahan adalah komponen penting dari upaya ini. Untuk menangani *deepfake*, pengembangan hukum internasional, kerja sama dengan platform online, pengembangan etika digital, dan dukungan kepada korban adalah komponen penting. Kita dapat melindungi masyarakat, mengurangi risiko *deepfake porn*, dan mencegah penyebaran konten yang merugikan dengan menerapkan pendekatan holistik yang melibatkan semua elemen ini.

Dengan hal itu, sangat penting untuk mendorong penelitian dan pengembangan teknologi yang lebih canggih untuk mendeteksi *deepfake*. Ini akan membantu mendeteksi *deepfake* dengan lebih akurat dan mengidentifikasi kontennya dengan lebih mudah. Dalam mengembangkan solusi ini, pemerintah, lembaga penelitian, dan industri teknologi dapat bekerja sama untuk memperkuat pertahanan kita terhadap penyebaran *deepfake*. Selain itu, transparansi dan akuntabilitas harus dibuat terkait penggunaan teknologi *deepfake* oleh pihak berwenang. Penegakan hukum dan lembaga pemerintah yang menggunakan teknologi *deepfake* dalam investigasi atau keamanan publik harus memiliki pedoman etis yang jelas. Hal ini akan membantu menjaga agar teknologi ini tidak disalahgunakan dan digunakan untuk kepentingan publik.

Oleh karena itu, kita dapat melindungi masyarakat dari ancaman *deepfake* dan menjaga integritas data digital dengan undang-undang yang kuat, teknologi identifikasi yang canggih, dan etika yang ketat saat menggunakan teknologi *deepfake*.Upaya lintas sektor yang holistik sangat penting untuk mencegah pornografi *deepfake* dan melindungi masyarakat dari bahayanya. Peraturan yang ketat dan efektif harus menjadi dasar penegakan hukum terhadap pelaku *deepfake*. Teknik identifikasi *deepfake* yang terus berkembang menjadi sarana penting untuk menemukan konten yang telah dimanipulasi. Sangat penting bagi upaya ini untuk melindungi korban, yang mencakup akses ke layanan hukum dan partisipasi masyarakat dalam melaporkan konten mencurigakan. Kolaborasi antar negara juga penting karena pelaku pornografi *deepfake* sering berasal dari berbagai negara. Pendidikan publik tentang keadaan digital dan evaluasi terus-menerus keberhasilan tindakan pencegahan adalah komponen penting dari upaya ini. Untuk menangani *deepfake*, pengembangan hukum internasional, kerja sama dengan platform online, pengembangan etika digital, dan dukungan kepada korban adalah komponen penting. Kita dapat melindungi masyarakat, mengurangi risiko pornografi *deepfake*, dan mencegah penyebaran konten yang merugikan dengan menerapkan pendekatan holistik yang melibatkan semua elemen ini. Penyebaran kesadaran publik yang luas akan membantu menemukan dan mengidentifikasi *deepfake*, sedangkan kolaborasi antar negara akan memungkinkan penerapan undang-undang yang lebih ketat dan hukuman yang lebih berat bagi mereka yang melanggarnya.

DAFTAR PUSTAKA

Peraturan Perundang-Undangan

Pasal 35, Undang-Undang No. 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Pasal 51, Undang-Undang No. 11 Tahun 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Peraturan Pemerintah Pengganti Undang-Undang No. 18 Tahun 1960 tentang Informasi dan Transaksi Elektronik (Indonesia). diakses 31 Oktober 2023, dari http://peraturan.bpk.go.id/Details/53472/perpu-no-18-tahun-1960

Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Indonesia). diakses 31 Oktober 2023, dari http://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016

Undang-Undang No. 36 Tahun 1999 tentang Perubahan Jumlah Hukuman Denda Dalam Kitab Undang-Undang Hukum Pidana Dan Dalam Ketentuan-Ketentuan Pidana Lainnya Yang Dikeluarkan Sebelum Tanggal 17 Agustus 1945 (Indonesia). diakses 31 Oktober 2023, dari http://peraturan.bpk.go.id/Details/45357/uu-no-36-tahun-1999

Buku

Baker, D. J., & Robinson, P. H. (2020). *Artificial Intelligence and the Law: Cybercrime and Criminal Liability*. Routledge.

Maskun. (2022). Kejahatan Siber (Cyber Crime): Suatu Pengantar. Prenada Media.

Meikle, G. (2022). Deepfakes. John Wiley & Sons. (Chapter 4).

Yurizal. (2018). Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia. Media Nusa Creative (MNC Publishing).

Lain-lain

Auli, Renata Christha. (2023). Apa Itu Deepfake Porn dan Jerat Pidana bagi Pelakunya. Diakses pada 31 Oktober 2023, Retrieved From https://www.hukumonline.com/klinik/a/apa-itu-deepfake-porn-dan-jerat-pidana-bagi-pelakunya-lt6530d3546d9c4/

Ayya Sofia Istifarrah, Pertanggungjawaban Pidana Pelaku Pendistribusian Konten Yang Bermuatan Asusila Melalui Media Elektronik (Universitas Airlangga 2020).

Hosnah, A. U., Antoni, H., & Yofany, R. (2023). Law Enforcement Against Perpetrators of Defamation Through Social Media Based on the ITE Law. International Journal of Multicultural and Multireligious Understanding, 10(4), 362–372. Retrieved 6 November 2023 from https://doi.org/10.18415/ijmmu.v10i4.4643

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? Business Horizons, 63(2), 135–146. Diakses pada 31 Oktober 2023, Retrieved From https://doi.org/10.1016/j.bushor.2019.11.006

Unpad, P. F. (2023). Perlindungan Hukum Bagi Korban DEEPFAKE Pornografi: Evaluasi Efektivitas Hukum Positif Dan Kebutuhan Akan Reformasi Hukum. Diakses dari https://pleads-fhunpad.medium.com/perlindungan-hukum-bagi-korban-deepfake-pornografi-evaluasi-efektivitas-hukum-positif-dan-1fb2bb20da35

“How AI Is Driving an Explosive Rise in Deepfake Pornography.” Euronews, 20 Oct. 2023, Retrieved From https://www.euronews.com/next/2023/10/20/generative-ai-fueling-spread-of-deepfake-pornography-across-the-internet.

Burgess, Matt. “Deepfake Porn Is Out of Control.” Wired. retrieved From www.wired.com, https://www.wired.com/story/deepfake-porn-is-out-of-control/.

Harris, Douglas. “Deepfakes: False Pornography Is Here and the Law Cannot Protect You.” Duke Law & Technology Review, vol. 17, no. 1, Jan. 2019, pp. 99–127, Retrieved From https://scholarship.law.duke.edu/dltr/vol17/iss1/4.