

ANALISIS TINDAK PIDANA *DEEPFAKE* PORNOGRAFI DALAM PERSPEKTIF UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK¹

Oleh :

Michelle Lucia Korengkeng²

Roy Ronny Lembong³

Feiby S. Wewengkang⁴

ABSTRAK

Penelitian ini bertujuan untuk mengetahui dan memahami pengaturan hukum terhadap tindak pidana *deepfake* pornografi berdasarkan Undang-Undang Informasi dan Transaksi Elektronik dan untuk menganalisis prospek penegakan hukum terhadap tindak pidana *deepfake* pornografi di Indonesia, khususnya dalam konteks perkembangan teknologi digital. Metode yang digunakan adalah yuridis normatif, dengan kesimpulan yaitu: 1. Pengaturan dalam Pasal 27 ayat (1) jo. Pasal 45 ayat (1) UU ITE memang mengandung larangan atas distribusi muatan yang melanggar kesusilaan, namun tidak secara eksplisit mengatur atau menyebut konten digital hasil manipulasi berbasis kecerdasan buatan seperti *deepfake*. Dalam praktiknya, penegakan hukum terhadap konten *deepfake* pornografi sering kali tidak berhasil karena pelaku menyembunyikan identitas melalui jaringan anonim atau beroperasi lintas negara, sementara aparat penegak hukum Indonesia masih memiliki keterbatasan dalam bidang digital forensik dan pelacakan identitas virtual. 2. *Deepfake* pornografi bukan hanya kejahatan terhadap kesusilaan, melainkan juga merupakan bentuk pelanggaran serius terhadap hak atas privasi, martabat, dan integritas psikologis seseorang. Dalam konteks ini, sistem hukum pidana Indonesia belum memiliki perangkat normatif dan teknis yang mampu memberikan perlindungan yang memadai bagi korban.

Kata Kunci : *deepfake*, *pornografi*, *ITE*

PENDAHULUAN

A. Latar Belakang

Saat ini manusia sangat bergantung dengan teknologi di berbagai aspek keseharian, hal ini tentunya dilakukan dengan menerapkan teknologi untuk memudahkan berbagai aktivitas. Melalui media sosial dan internet, merupakan saluran utama yang dimanfaatkan. Melalui platform ini,

seseorang dapat terhubung dengan teman-teman, bahkan dengan individu asing yang tidak dikenal, yang tinggal di luar desa, kota, yang berbeda pulau maupun yang berbeda negara.

Salah satu perkembangan teknologi yang ada saat ini, bermula dari sistem pada komputer model statistic, yang digunakan untuk mengambil keputusan dengan menggeneralisir karakteristik dari suatu objek berbasis data yang kemudian dipasang di berbagai perangkat elektronik yang digunakan untuk mempercepat dan mempermudah kinerja dari manusia itu sendiri, hal ini menimbulkan sesuatu yang dinamakan *artificial intelligence*. *Artificial Intelligence* juga dapat didefinisikan dalam pengertian teknis sebagai penerapan algoritma dalam pengolahan data, identifikasi pola, pengambilan keputusan, dan bahkan prediksi hasil jangka panjang atau di masa depan.

Salah satu perkembangan teknologi yang belakangan menjadi perhatian global adalah hadirnya teknologi kecerdasan buatan (*Artificial Intelligence/AI*), yang salah satu penerapannya adalah dalam bentuk *deepfake*. Teknologi *deepfake* memungkinkan seseorang memanipulasi data visual atau audio, sehingga menciptakan rekaman video, foto, atau suara yang terlihat dan terdengar seolah-olah asli, padahal sesungguhnya palsu. Dengan menggunakan algoritma *deep learning*, wajah seseorang dapat ditempelkan ke tubuh orang lain dalam video dengan tingkat realisme yang tinggi, menjadikan hasilnya sulit dibedakan dari konten asli. Teknologi informasi dan komunikasi juga telah mengubah perilaku dan pola hidup masyarakat secara global, dan menyebabkan dunia menjadi tanpa batas (*borderless*), serta menimbulkan perubahan di berbagai bidang kehidupan.⁵

Dalam banyak kasus, wajah korban, terutama perempuan, diedit dan ditempelkan ke tubuh dalam video atau gambar pornografi, lalu disebarluaskan ke publik tanpa seizin korban. Bentuk kejahatan ini dikenal dengan istilah *deepfake* pornografi, dan merupakan salah satu bentuk kekerasan seksual digital yang sangat merusak martabat, privasi, dan reputasi seseorang.

Sosial media mempermudah pelaku kejahatan untuk mendapatkan data pribadi foto dan memanipulasinya menjadi gambar, foto, atau bahkan video baru yang terlihat seperti asli namun tidak sesuai dengan tempat, waktu, dan kondisi

¹ Artikel Skripsi

² Mahasiswa Fakultas Hukum Unsrat, NIM 20071101395

³ Dosen Fakultas Hukum Unsrat, Doktor Ilmu Hukum

⁴ Dosen Fakultas Hukum Unsrat, Magister Ilmu Hukum

⁵ Agus Raharjo, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung, 2002, hlm.34.

yang sesungguhnya.⁶ Ada keahlian khusus yang diperlukan untuk meniru foto dan foto sehingga terlihat seperti asli. Artificial intelligence mempermudah proses tersebut melalui web atau aplikasi tertentu yang memiliki fitur tertentu.⁷

Di Indonesia, fenomena ini mulai muncul dalam beberapa tahun terakhir, seiring meningkatnya penggunaan media sosial, aplikasi editing video, dan kemudahan akses teknologi digital. Namun, hingga kini, belum ada satu pun regulasi nasional yang secara tegas dan eksplisit mengatur mengenai kejahatan *deepfake* pornografi.

Penindakan terhadap pelaku masih mengandalkan ketentuan umum yang terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), sebagaimana telah diubah melalui UU Nomor 19 Tahun 2016, serta sebagian dari Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi. Sayangnya, kedua undang-undang tersebut belum secara eksplisit mengatur tentang konten pornografi hasil manipulasi digital yang menyerupai korban, tanpa keterlibatan fisik korban dalam pembuatan konten tersebut.

Ketentuan dalam Pasal 27 ayat (1) UU ITE memang mengatur larangan terhadap pendistribusian, penyiaran, dan/atau penyimpanan informasi elektronik atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan. Namun, ketentuan tersebut masih bersifat umum, dan belum dapat mengakomodasi karakteristik khusus dari konten *deepfake*, khususnya dalam hal pembuktian keterlibatan pelaku, ketiadaan unsur fisik korban, serta sifat manipulatif dari konten yang digunakan. Dalam banyak kasus, video *deepfake* tidak melibatkan tubuh atau suara asli korban, sehingga menimbulkan perdebatan apakah konten tersebut benar-benar memenuhi unsur “pornografi” atau “muatan melanggar kesusilaan” sebagaimana dimaksud dalam hukum positif Indonesia. Selain itu, proses penegakan hukum terhadap pelaku kejahatan *deepfake* pornografi juga menghadapi banyak tantangan, mulai dari kesulitan identifikasi pelaku yang sering kali menggunakan jaringan anonim, lokasi pelaku yang berada di luar negeri, hingga minimnya kemampuan forensik digital aparat penegak hukum di Indonesia. Tantangan ini semakin diperparah oleh fakta bahwa penyebaran konten digital dapat berlangsung sangat cepat dan

masif, sehingga menyebabkan kerugian psikologis dan sosial yang besar sebelum korban sempat melakukan langkah hukum.

Dari sisi regulasi, Indonesia juga belum memiliki instrumen hukum yang secara spesifik mengatur pertanggungjawaban pelaku teknologi, seperti pengembang aplikasi, penyedia platform media sosial, atau perusahaan teknologi yang menyediakan alat atau layanan yang memungkinkan pembuatan konten *deepfake*. Padahal, dalam sistem hukum pidana modern, konsep pertanggungjawaban pidana korporasi dan delik teknologi telah menjadi bagian penting dalam upaya mengimbangi kemajuan teknologi informasi.

Melihat realitas tersebut, Indonesia perlu segera melakukan penyesuaian terhadap peraturan perundang-undangan yang ada. Tanpa pembaruan hukum yang relevan, aparat penegak hukum tidak akan memiliki pijakan hukum yang kuat untuk menjerat pelaku kejahatan *deepfake* pornografi secara adil dan tuntas. Selain itu, keterlambatan negara dalam merespons fenomena ini dapat berujung pada krisis kepercayaan masyarakat terhadap sistem hukum, terutama bagi korban perempuan yang paling sering menjadi sasaran konten pornografi digital. Dengan demikian, penting untuk mengkaji secara yuridis posisi dan efektivitas UU ITE sebagai dasar hukum dalam menanggulangi kejahatan *deepfake* pornografi, baik dari segi rumusan normatif, ruang lingkup subjek hukum, efektivitas sanksi, hingga peluang pembaruan legislasi yang lebih adaptif terhadap perkembangan teknologi.

Fenomena *deepfake* pornografi tidak hanya menimbulkan persoalan hukum semata, tetapi juga mencerminkan adanya kegagalan perlindungan hak asasi manusia, terutama hak atas privasi, kehormatan, dan perlindungan terhadap kekerasan berbasis gender. Korban *deepfake* pornografi kerap mengalami diskriminasi, stigma sosial, serta tekanan psikologis yang mendalam akibat konten yang tidak pernah mereka setuju tersebut tersebar luas di dunia maya. Oleh karena itu, peran hukum tidak hanya sebatas memberikan sanksi pidana kepada pelaku, melainkan juga memberikan perlindungan efektif kepada korban.

Namun, dalam konteks hukum Indonesia, perlindungan terhadap korban *deepfake* pornografi masih sangat terbatas. Ketentuan yang ada di UU ITE dan Undang-Undang Pornografi belum secara spesifik mengatur mengenai teknologi rekayasa digital yang dapat memproduksi dan menyebarkan konten bermuatan pornografi tanpa harus melibatkan korban secara fisik. Ini menimbulkan celah

⁶ Renata, “Aspek Hukum Perlindungan Data Pribadi Source Subject Terhadap Penggunaan Teknik Deepfake Dalam Perspektif Perbuatan Melanggar Hukum.”, (Indralaya: Fakultas Hukum Universitas Sriwijaya, 2022). 22

⁷ Ibid, 23

hukum yang berpotensi dimanfaatkan oleh pelaku untuk menghindari pertanggungjawaban pidana. Kekosongan norma tersebut menjadi tantangan besar, mengingat kemajuan teknologi yang begitu cepat membawa dampak nyata dalam kehidupan sosial dan hukum. Dalam konteks ini, hukum pidana harus mampu menyeimbangkan antara kemajuan teknologi dengan perlindungan hak asasi manusia, agar teknologi tidak menjadi alat pelanggaran dan eksploitasi. Pendekatan hukum yang adaptif dan progresif sangat diperlukan untuk mengantisipasi perkembangan teknologi yang terus berubah, termasuk dalam ranah *deepfake* pornografi.

B. Rumusan Masalah

1. Bagaimana pengaturan hukum terhadap *deepfake* pornografi dalam perspektif undang-undang informasi dan transaksi elektronik?
2. Bagaimana prospek terhadap tindak pidana *deepfake* pornografi?

C. Metode Penelitian

Dalam penelitian ini, penulis menggunakan metode penelitian hukum normatif.

PEMBAHASAN

A. Pengaturan Hukum Terhadap *Deepfake* Pornografi Dalam Perspektif Undang-Undang Informasi Dan Transaksi Elektronik

Negara Indonesia sendiri, saat ini sangat marak dengan kasus hoax atau penipuan dengan memanfaatkan teknologi *deepfake* untuk membuat dan menyebarkan foto/video orang yang menjadi targetnya. Hal ini diproses sedemikian rupa agar terlihat sangat nyata dan tentunya ini mengandung unsur pornografi. Pornografi sendiri berasal dari kata "*pornographic*" yang berasal dari bahasa Yunani yaitu *pornographos* (*porne*= pelacur, dan *graphien*= tulisan atau lukisan, jadi tulisan atau lukisan tentang pelacur, atau suatu deskripsi dari perbuatan para pelacur). Gambar atau tulisan tentang pelacur, kadang-kadang juga disingkat menjadi "porn", "pr0n", atau "porno", adalah gambar tubuh manusia atau perilaku seksualitas manusia secara terbuka dengan tujuan menimbulkan gairah seksual.⁸ Berdasarkan definisi ini segala karya manusia baik berupa cerita, gambar, film, tarian maupun lagu yang diciptakan dengan maksud sengaja untuk membakar nafsu birahi orang lain, sehingga merangsang syahwatnya serta menimbulkan

pikiran-pikiran jorok dibenaknya.⁹ Jadi pornografi berarti tulisan, gambar, patung atau barang pada umumnya yang menggambarkan sesuatu yang menyinggung rasa susila bagi setiap orang yang membaca atau melihatnya.¹⁰

Melalui suatu proses editing yang sedemikian rupa, gambar-gambar yang berbeda yang diproses sehingga dapat dengan mudah untuk disatukan dan menghasilkan suatu foto/video yang baru. Teknik *deepfake* pada gambar dengan cara mengubah ekspresi wajah, wajah, atau tubuh seseorang dalam foto atau gambar aslinya untuk membuat gambar baru yang realistis, bahkan sulit dibedakan dengan mata manusia. Proses ini menggunakan analisis atau pembelajaran mendalam lewat *artificial intelligence* untuk menghasilkan gambar baru dengan ekspresi wajah, atau wajah seseorang dengan tubuh yang berbeda dari foto atau gambar aslinya. *Artificial intelligence* ini bekerja melalui sistem *machine learning*, pada *machine learning* proses di mana komputer tanpa pemrograman eksplisit dilatih untuk "belajar" dari data, dan membuat prediksi atau menghasilkan konten baru. Pembuatan *deepfake Model Generative Adversarial Networks* (GAN) adalah salah satu teknik paling canggih yang digunakan untuk menghasilkan sebuah *deepfake*.

Deepfake pornografi adalah jenis kejahatan digital atau cybercrime, yang menggabungkan elemen pornografi ilegal dengan teknologi manipulasi visual berbasis kecerdasan buatan. Ancama yang ditimbulkan oleh kejahatan siber menjadi tantangan bagi pemerintah karna sulit untuk melawan teknik kejahatan yang semakin canggih. Pornografi merupakan salah satu contoh kejahatan siber yang terjadi di Indonesia saat ini.¹¹ Tindak pidana dalam *deepfake* pornografi memiliki beberapa karakteristik yang membedakannya dari jenis kejahatan lain:

- 1) *Deepfake* pornografi berbasis teknologi kecerdasan buatan menggunakan *Artificial intelligence* untuk mengganti wajah korban dengan tubuh atau adegan seksual yang sudah ada.
- 2) Tanpa keterlibatan fisik korban, salah satu fitur paling berbahaya dari pornografi *deepfake* adalah bahwa korban tidak pernah

⁸ <https://id.wikipedia.org/wiki/Pornografi> diakses pada Mei 2025

⁹ Tjipta Lesmana, *Pornografi Dalam Media Massa*, Puspa Swara. Jakarta. 1995. hal 107.

¹⁰ Wirjono Prodjodikoro, *Tindak Pidana Tertentu di Indonesia*, PT. Rafika Aditama, Bandung, 2003, hal 78.

¹¹ Eva Istia Utawi, Neni Ruhaeni, "Penegakan Hukum Terhadap Tindak Pidana Pornografi Menurut Peraturan Perundang-Undangan Tentang Pornografi Melalui Media Sosial" *Bandung Conference Series: Law Studies*, Vol.3 No.1, (2023), 365.

terlibat secara fisik dalam aktivitas seksual, wajah, bahkan suara dari korban digunakan tanpa izin.

- 3) Tersebar melalui media digital, biasanya konten-konten yang bermuatan pornografi *deepfake* ini diunggah atau disebarluaskan secara meluas melalui internet.
- 4) Sulit dideteksi atau bahkan diidentifikasi, bukti *deepfake* sulit dibedakan dari kebenaran karena realistis dan mirip dengan konten asli. Untuk memastikan bahwa video atau foto tersebut telah dimanipulasi dan untuk mengidentifikasi orang yang melakukannya, diperlukan keahlian digital forensik.
- 5) Potensi pelaku dari negara lain dan anonim, penegakan hukum menjadi lebih kompleks karena pelaku *deepfake pornografi* dapat berasal dari negara lain dan menggunakan identitas anonim. Ini mengganggu yurisdiksi dan ekstradisi selama proses peradilan dan penyidikan yang ada.

Titik berat dari keberadaan *deepfake* porn ini yaitu terletak pada pihak-pihak yang memanfaatkan perkembangan teknologi AI dengan salah untuk membuat *deepfake* porn. Menitik beratkan keberadaan *deepfake* porn kepada manusia dikarenakan antara manusia dan teknologi memiliki perbedaan. Teknologi tidak terikat oleh batasan moral sementara manusia memiliki kemampuan untuk melakukan tindakan-tindakan yang sesuai dengan prinsip-prinsip moral, hukum, dan lingkungan sosial.¹² Teknologi AI hanya melakukan suatu proses sesuai dengan apa yang diperintahkan oleh manusia.

Berdasarkan pada Pasal 27 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan UU Nomor 19 Tahun 2016 berbunyi: “setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan”.

Dari bunyi Pasal 27 ayat (1) UU 1/2024, terdapat beberapa penjelasan atas unsur pasal sebagai berikut:

1. “Menyiarkan” termasuk perbuatan mentransmisikan, mendistribusikan, dan membuat dapat diaksesnya informasi dan/atau dokumen elektronik dalam sistem elektronik.

2. “Mendistribusikan” adalah mengirimkan dan/atau menyebarkan informasi dan/atau dokumen elektronik kepada banyak orang atau berbagai pihak melalui sistem elektronik.
3. “Mentransmisikan” adalah mengirimkan informasi dan/atau dokumen elektronik yang ditujukan kepada pihak lain melalui sistem elektronik.
4. “Membuat dapat diakses” adalah semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui sistem elektronik yang menyebabkan informasi dan/atau dokumen elektronik dapat diketahui pihak lain atau publik.
5. “Melanggar kesusilaan” adalah melakukan perbuatan mempertunjukkan ketelanjangan, alat kelamin, dan aktivitas seksual yang bertentangan dengan nilai-nilai yang hidup dalam masyarakat di tempat dan waktu perbuatan tersebut dilakukan penafsiran pengertian kesusilaan disesuaikan dengan standar yang berlaku pada masyarakat dalam waktu dan tempat tertentu (*contemporary community standard*).
6. “Diketahui umum” adalah untuk dapat atau sehingga dapat diakses oleh kumpulan orang banyak yang sebagian besar tidak saling mengenal.¹³

Lebih lanjut lagi, pada pasal 27 ayat (1) ini ada hal-hal yang menjadi bagian unsur penting terutama dalam *deepfake* pornografi :

- Unsur perbuatan, perbuatan disini yaitu kegiatan mendistribusikan, mentransmisikan atau kegiatan membuat dapat diaksesnya *deepfake* pornografi.
- Unsur tanpa hak dan dengan sengaja
- Unsur objek, objek disini berupa informasi elektronik dan/atau dokumen elektronik
- Unsur muatan, dalam hal ini yang mengandung kesusilaan

Oleh karena itu, dalam kasus penyebaran konten palsu melalui *deepfake* UU ITE dapat diterapkan sebagai hukum khusus yang mengatur transaksi elektronik, termasuk distribusi konten pornografi yang menggunakan teknologi *deepfake*, melecehkan atau memfitnah.¹⁴

¹² Andhika Nugraha Utama, Prama Tusta Kesuma, and Rio Maulana Hidayat, “Analisis Hukum Terhadap Upaya Pencegahan Kasus Deepfake Porn Dan Pendidikan Kesadaran Publik Di Lingkungan Digital,” *Jurnal Pendidikan Tambusai* 7, no. 3 (2023): 26179–88.

¹³ Penjelasan Pasal 27 ayat (1) Undang-Undang Nomor 11 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (“UU 1/2024”)

¹⁴ Zenifa Siti Hafsyari, dkk. “Korban Deepfake Pornografi Evaluasi Efektivitas Hukum Positif Dan Kebutuhan akan Reformasi Hukum”. Dalam <https://pleads.fhunpad.medium.com/perlindungan-hukum-bagi-korban-deepfake-pornografi-evaluasi-efektivitas-hukum-positif-dan-1fb2bb20da35> Di akses 15 april 2025

Pasal 27 ayat (1) digunakan untuk mejerat para pelaku penyebaran konten pornografi secara digital, karena pornografi secara umum dianggap sebagai bagian dari muatan yang melanggar kesusilaan. Namun, penafsiran kata “melanggar kesusilaan” masih bersifat umum dan terbuka.

Lebih lanjut “melanggar kesusilaan” Dalam UU ITE, istilah “kesusilaan” tidak didefinisikan secara eksplisit. Namun, dalam hukum Indonesia, istilah “kesusilaan” sering didefinisikan sebagai norma atau kaidah yang mengatur tingkah laku yang sesuai dengan standar moral masyarakat, terutama yang berkaitan dengan seksualitas, sopan santun, dan etika hubungan antarpribadi.

Tidak hanya itu Mahkamah Konstitusi (MK) memiliki penafsiran dalam putusan MK No. 50/PUU-VI/2008, MK menyatakan bahwa “muatan melanggar kesusilaan” dapat mencakup ajakan, gambar, atau informasi tentang aktivitas seksual yang tidak sesuai dengan norma masyarakat Indonesia.

Kaitan melanggar kesusilaan dengan pornografi digital yaitu karena pornografi digital ini disebarkan melalui media internet, maka dari itu pornografi digital dikategorikan sebagai suatu hal yang “melanggar kesusilaan”. Cakupan dari pornografi digital ini sangatlah luas termasuk gambar, video, GIF, maupun manipulasi wajah dan suara seperti kasus yang marak ini terjadi seperti kasus *deepfake*.

Pornografi *deepfake* ini memang pada dasarnya tidak disebutkan secara eksplisit dalam pasal 27 ayat (1) undang-undang Informasi dan Transaksi Elektronik, tetapi secara substansial pornografi *deepfake* termasuk kedalam cakupan undang-undang ini. *Deepfake* pornografi ini memiliki unsur “muatan melanggar kesusilaan” dalam *deepfake* pornografi menampilkan hasil manipulasi seseorang dengan adegan seksual yang terlihat sangat realistis dan tentunya ini memiliki muatan “mengandung asusila”, penggunaan wajah asli dari seseorang kedalam adegan pornografi hasil rekayasa juga “melanggar kesusilaan, privasi, dan kehormatan pribadi” dari korban.

Selanjutnya unsur “mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya”, dalam hal *deepfake* pornografi biasanya pelaku menyebarluaskan hasil manipulasinya melalui media internet (media sosial, situs dewasa, bahkan grup pesan) dengan hal ini pelaku memenuhi unsur “distribusi elektronik” dalam pasal 27 ayat (1) UU ITE. Selanjutnya unsur, “dengan sengaja dan tanpa hak” dalam pembuatan dan penyebaran konten *deepfake* pelakunya tahu bahwa mereka

menggunakan citra dari orang lain tanpa izin dan tahu bahwa konten tersebut bermuatan asusila.

Hal ini menunjukkan itikat tidak baik (*mens rea*) dengan perbuatan yang sadar orang tersebut memenuhi unsur kesengajaan. Maka dengan itu jelas bahwa pornografi termasuk dalam cakupan pasal 27 ayat (1) undang-undang Informasi dan Transaksi Elektronik. Dalam beberapa dekade terakhir, kemajuan perkembangan teknologi digital khususnya kecerdasan buatan (*Artificial Intelligence*) dan pembelajaran mesin (*machine learning*) telah berkembang lebih cepat daripada kemampuan hukum untuk mengantisipasi dan mengontrol efeknya. Ini telah menyebabkan perbedaan antara praktik teknologi dan konstruksi hukum yang mengaturnya.

Jenis sanksi pidana terhadap pelanggaran hukum digital, termasuk konten yang melanggar kesusilaan seperti *deepfake* pornografi, diatur oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), sebagaimana telah diubah dengan UU Nomor 19 Tahun 2016 yang mengatur jenis-jenis sanksi pidana yang terbagi menjadi pidana pokok dan pidana tambahan. Dalam konteks penyebaran konten *deepfake* pornografi, beberapa pasal relevan antara lain pasal 27 ayat (1), pasal 29, dan pasal 45b.

Berdasarkan sanksi pasal (45 ayat 1) menjadi dasar utama penindakan atas pelaku penyebaran konten *deepfake* pornografi, karena konten tersebut dapat dikualifikasikan sebagai muatan melanggar kesusilaan. Dalam hal ini, memiliki kelebihan jangkauan yang sangat luas dan bisa menjangkau distribusi konten pornografi *deepfake*. Kekurangannya tidak secara eksplisit mengatur konten hasil manipulasi *deepfake* dan interpretasi “melanggar kesusilaan” bisa subjektif.

Berdasarkan pasal 29 UU ITE, pasal ini dapat digunakan jika konten *deepfake* digunakan untuk memeras atau mengancam korban (contohnya, “Jika anda tidak membayar, video ini akan disebarkan”). Kekurangannya hanya berlaku jika ada unsur ancaman langsung, maka dari itu tidak selalu cocok untuk semua kasus *deepfake* pornografi.

Berdasarkan hal tersebut, aspek represifitas relatif cukup dalam bentuk ancaman hukuman tapi belum menyasar teknologi *deepfake* secara spesifik. Dalam sanksi ini kurang optimal dalam memberikan efek jera bagi pelaku, disebabkan oleh rendahnya penegakan hukum juga pelaku sering sulit untuk dilacak karena menggunakan identitas palsu atau dari luar negeri, beserta kurang pahamiannya aparat tentang teknologi *deepfake*.

Sanksi dalam UU ITE tidak sepenuhnya relevan untuk pelaku yang menggunakan teknologi *Artificial Intelligence*, karna dalam undang-undang ITE belum cukup spesifik untuk menjangkau kompleksitas kejahatan berbasis teknologi tinggi seperti *deepfake* yang berbasis *Artificial Intelligence*. Isi dari cakupan UU ITE terbatas pada pasal yang digunakan.

- Pasal 27 ayat (1) soal “muatan yang melanggar kesusilaan”
- Pasal 29 soal ancaman kekerasan/mengintimidasi korban
- Pasal 25b soal pidana untuk pelanggaran tersebut

Tetapi, tidak ada pengaturan eksplisit mengenai;

- Konten hasil manipulasi teknologi (AI/*deepfake*)
- Rekayasa citra digital, meskipun tanpa konten seksual eksplisit
- Perbedaan pelaku pembuat, penyebar, dan penyimpan

UU ITE mengandalkan istilah “kesusilaan” atau “penghinaan”, yang sulit diinterpretasikan untuk konten berbasis teknologi AI modern. Selanjutnya, dalam relevannya sanksi bagi pelaku terdapat kejahatan yang tidak terakomodir dikarenakan karakteristik dari *Artificial Intelligence* itu sendiri.

- Karakteristik anonitis dan global, dalam hal ini UU ITE tidak responsif, karena pelaku tak terlacak atau bahkan lintas negara
- Karakteristik manipulasi visual realistis, UU ITE tidak spesifik responsif, karna tidak ada aturan tentang konten palsu yang menyerupai seseorang.
- Karakteristik viralitas konten, UU ITE terbatas dalam responsif, karna tidak mempertimbangkan efek jangka panjang dari distribusi cepat *deepfake*.
- Karakteristik pembuat konten tanpa menyebarkan, pada UU ITE belum diatur karna UU ITE berfokus pada “penyebab”

Oleh karena itu, beberapa karakteristik yang muncul karena kejahatan AI tidak terakomodasi dengan baik dalam undang-undang ITE. Selanjutnya, dalam hal relevannya sanksi dalam UU ITE. Sanksi dan dampak tidak seimbang, sanksi pornografi *deepfake* dapat menyebabkan kerusakan reputasi, trauma psikologis, dan penggunaan pemerasan atau pelecehan. Namun, tanpa memperhitungkan tingkat kerusakan, niat jahat dalam desain AI, dan kemungkinan penyebaran massal, ancaman hukumnya masih berkisar 6 tahun penjara saja. Dengan demikian, sanksi tersebut tidak cukup menciptakan efek jera,

terutama untuk pelaku yang memiliki kemampuan teknis tinggi dan dapat menghindari pelacakan hukum.

Sementara itu dalam hal pertanggungjawaban pelaku pada UU ITE terkait *deepfake* pornografi, pada pertanggungjawaban pelaku perorangan cukup memadai karna UU ITE mengaturnya secara eksplisit terutama dalam cakupan pasal 27 ayat (1), pasal 29, dan pasal 45 dan 45b.

Salah satu kelemahan utama UU ITE adalah kekurangan standar, terutama dalam hal istilah dan definisi hukum yang berkaitan dengan kemajuan teknologi baru, seperti *deepfake*. Meskipun bisa dijangkau secara implisit, pendekatan ini menyimpan sejumlah kelemahan :

- a. Undang-undang ITE belum responsif terhadap inovasi teknologi UU ITE, revisi UU No. 19 Tahun 2016 belum mengakomodasi perkembangan teknologi seperti “*Artificial Intelligence*”, *machine learning*, atau bahkan *deepfake*. Baik batang tubuh maupun penjelasan UU ITE tidak mengandung istilah seperti “manipulasi digital visual”, “media sintetis”, atau “konten berbasis AI”.
- b. Ketidakpastian Hukum (Legal Uncertainty) akibat kekosongan terminologi aparat penegak hukum harus menggunakan pasal-pasal umum, seperti Pasal 27 ayat (1) tentang kesusilaan atau Pasal 28 tentang berita bohong, untuk interpretasi yang luas. Aparat penegak hukum harus menafsirkan elemen-elemen pasal secara menyeluruh karena tidak secara khusus mengatur *deepfake*. Sehubungan dengan frasa “Muatan Melanggar Kesusilaan” yang terdapat dalam Pasal 27 ayat (1) UU ITE, kata-kata seperti “kesusilaan”, “tanpa hak”, dan “dapat diakses” dapat ditafsirkan dengan berbagai cara.

Terdapat perbedaan interpretasi antara penegak hukum tentang *deepfake* karena konten asusila yang dihasilkan dari manipulasi visual mungkin tidak dianggap sebagai pornografi biasa. Hal ini dapat menyebabkan penegak hukum berbeda-beda memahami sanksi dan tidak konsisten, dalam menerapkannya tergantung pada sudut pandang penyidik, hakim, atau jaksa.

- c. Masalah Pembuktian *deepfake* adalah konsekuensi dari manipulasi visual yang kompleks yang sulit dideteksi tanpa alat deteksi digital atau bantuan forensik digital. Unsur “kesengajaan” dan “tanpa hak” juga sulit dibuktikan jika pelaku menggunakan akun anonim, atau bahkan beroperasi di luar negeri dan pelaku menyembunyikan jejak

digital melalui VPN atau melalui dark web. Tidak adanya standar teknis pembuktian untuk konten manipulatif dalam UU ITE dapat menghambat proses hukum ini.

- d. Tidak ada undang-undang pencegahan UU ITE, yang berarti hanya bertindak setelah tindak pidana terjadi. Belum ada aturan yang mengatur cara mencegah atau menanggapi penyebaran konten *deepfake*. Sistem seperti sistem pelaporan, verifikasi, atau pelabelan konten belum ada.

Karena UU ITE tidak mencantumkan istilah, objek hukum, atau persyaratan teknis yang berkaitan dengan konten manipulasi berbasis AI, beberapa pasalnya masih dapat digunakan untuk menjerat pelaku, terutama jika konten memiliki konten yang melanggar kesusilaan atau merugikan korban. Meskipun begitu, penegakan hukum implisit tidak kuat dan menimbulkan ketidakpastian hukum.

Untuk mengisi kekosongan yang tidak terpenuhi dalam UU ITE, perlu dipertimbangkan bagaimana undang-undang lain menyediakan alternatif atau pelengkap secara normatif.

Menurut Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, pornografi mencakup gambar, tulisan, suara, film, video, dan bentuk komunikasi lain yang menggambarkan atau mengeksploitasi aktivitas seksual. Meskipun UU Pornografi tidak menyebutkan istilah "*deepfake*", definisinya luas dan dapat digunakan untuk menjerat konten *deepfake* yang mengandung unsur eksploitasi seksual. Kelemahan undang-undang ini lebih menekankan pada pelaku pembuatan konten secara fisik, kurang relevan untuk kasus yang hanya melibatkan manipulasi visual tanpa korban yang terlibat secara langsung.

Disisi lain, Undang-undang Nomor 22 Tahun 2022 tentang Perlindungan Data Pribadi. Data biometrik seperti wajah, suara, dan ekspresi termasuk dalam kategori data sensitif yang didefinisikan dalam UU PDP. Penggunaan data biometrik seseorang untuk membuat *deepfake* tanpa izin dapat melanggar hak atas privasi dan perlindungan data pribadi. Oleh karena itu, UU PDP dapat digunakan untuk melindungi korban *deepfake* dari penyalahgunaan data pribadinya. Ini berlaku meskipun UU Pornografi atau UU ITE tidak memberikan sanksi pidana yang keras.

Sementara itu, efektivitas penegakan hukum dalam kasus internasional yang terjadi pada negara Korea Selatan dalam penindakan sangatlah progresif sejak tahun 2021, di Korea Selatan banyak kasus yang terjadi. Kasus pelaku pembuat dan penyebar konten *deepfake* dengan wajah selebritis Korea, seperti aktris atau idol K-

pop. Pemerintah Korea Selatan dalam menyikapi kasus *deepfake* pornografi menetapkan larangan tegas terhadap pembuatan dan penyebaran konten seksual *deepfake*. Pelaku dijera dengan hukuman hingga 5 tahun penjara. Korea Selatan juga mewajibkan platform menghapus konten dalam waktu 24 jam setelah laporan. Penegakan hukum berlangsung aktif dengan sejumlah pelaku dihukum meski hanya menyebarkan, bukan membuat. Dalam hal ini, regulasi yang spesifik ditambah penegakan yang cepat memberikan efek jera. Hal inilah yang menjadikan Korea Selatan sebagai acuan global dalam penegakan kejahatan seksual digital, termasuk juga didalam ini penggunaan *Artificial Intelligence*.

B. Prospek Terhadap Tindak Pidana Deepfake Pornografi

Penegakan hukum terhadap tindak pidana *deepfake* pornografi menghadapi hambatan yang signifikan, baik dari segi teknis, hukum, maupun sumber daya manusia. Karakteristik kejahatan ini yang berbasis teknologi tinggi dan bersifat tersembunyi (*invisible crime*) menjadikannya sulit ditangani melalui pendekatan hukum konvensional.

Penegakan hukum dalam menangani tindak pidana *deepfake* pornografi menghadapi tantangan signifikan dari sudut pandang substansi hukum, serta masalah kelembagaan dan teknis. Cybercrime jenis baru ini membutuhkan tanggapan yang cermat, cepat, dan berbasis teknologi.

Dalam penegakan hukum kasus *deepfake* pornografi terdapat tantangan teknis dalam proses pembuktian :

1. Forensik Digital, seperti yang sudah disebutkan sebelumnya forensik digital sangatlah penting dalam pembuktian suatu konten hasil manipulasi (*deepfake*) . Tantangan utamanya berupa :
 - Teknologi *deepfake* sangatlah realistis ini sangatlah sulit untuk diidentifikasi oleh mata manusia
 - Dalam menganalisisnya proses pembuktian membutuhkan waktu yang sangatlah Panjang dan lama sehingga menghambat proses hukum.
 - Kurangnya alat deteksi khusus, dalam hal ini di Indonesia sendiri hanya laboratorium tertentu yang memiliki *software* pendeteksi konten sintesis (misalnya Microsoft Video Authenticator atau Deepware Scanner)

2. Identifikasi dan pelacakan pelaku, dalam identifikasi maupun pelacakan pelaku *deepfake* masalah yang muncul antara lain :
 - Mengakses internet melalui VPN atau menggunakan proxy server luar negeri
 - Pelaku menggunakan akun anonim atau identitas palsu
 - Menyebarkan konten melalui platform yang tidak tunduk pada hukum Indonesia (situs luar negeri, dark web, telegram).

Lebih lanjut dalam hal ini kesiapan dari aparat penegakan hukum sangatlah diperlukan, terlebih dalam menyikapi dan menindak kasus *deepfake* pornografi di Indonesia. Unsur-unsur yang kiranya dibutuhkan dalam hal ini :

1. Polri dan penyidik Siber, Indonesia memang telah membentuk divisi *Cyber Crime* Bareskrim Polri namun sejauh ini divisi ini lebih berfokus pada kasus-kasus penipuan online, pencemaran nama baik, serta pornografi konvensional. Ini menyebabkan penegakan *deepfake* membutuhkan SDM teknis yang paham mengenai *Artificial Intelligence* dalam pemrosesan citra digital, kolaborasi lintas sektor juga dibutuhkan (ahli hukum, teknologi, psikolog), juga dibutuhkan perangkat lunak yang bisa mendeteksi suatu konten *deepfake*.
2. Kejaksaan dan Pengadilan, dalam proses persidangan, bukti digital yang menunjukkan konten *deepfake* sering tidak diterima jika dalam pembuktiannya tidak ada prosedur verifikasi standar dan bukti diambil tanpa rantai elektronik (*chain of custody*) yang sah. Hakim juga jaksa juga sering tidak memahami teknis mendalam untuk mengevaluasi hasil analisis *deepfake* sehingga putusan hakim dalam argumentasi teknologi.
3. Ketergantungan pada pelaporan korban, banyak korban *deepfake* tidak menyadari bahwa mereka telah dimanipulasi dalam konten pornografi. Ketakutan akan stigma sosial dan kesulitan mengakses keadilan membuat sebagian korban enggan melapor, sehingga banyak kasus tidak terdeteksi dan tidak ditangani.

Dalam kasus *deepfake* pornografi, penegakan hukum menghadapi banyak masalah kelembagaan dan teknis. Pencegahan *deepfake* membutuhkan pendekatan holistik yang mencakup edukasi, pengembangan teknologi pendeteksian, peraturan hukum, dan kerja sama internasional.¹⁵ Banyak kasus tidak dapat ditangani karena aparat tidak

siap untuk forensik digital, identifikasi pelaku, dan interpretasi hukum berbasis teknologi. Diperlukan reformasi mendalam dalam regulasi, peningkatan sumber daya manusia, infrastruktur pendukung, dan kolaborasi antarnegara dan lintas sektor.

Pada kasus *deepfake* pornografi korban umumnya tidak melaporkan karena merasa malu bahkan tidak percaya pada aparat penegak hukum, dalam hal ini polisi atau bahkan jaksa tidak mampu membuktikan unsur “kesusilaan” atau “niat jahat” (*mens rea*) karena pelaku sering anonim, juga pada yurisprudensi lintas negara terbatas di Indonesia karena banyak pelaku atau situs tidak bisa disentuh.¹⁶

Kendala penegakan hukum Indonesia disini muncul :

- 1) Pembuktian dan Niat Jahat (*Mens Rea*)
Sulit membuktikan niat menyebarkan untuk mencemarkan atau merusak, karena pelaku bisa mengklaim hanya “iseng” atau “untuk hiburan”. Pembuatan *deepfake* bisa dilakukan secara otomatis tanpa proses manual intensif.
- 2) Bukti Digital dan Forensik
Forensik digital Indonesia masih terbatas dalam proses identifikasi metadata dan sumber AI sering tidak bisa dilakukan tanpa kerja sama platform luar.
- 3) Yurisprudensi Lintas Negara
Banyak konten *deepfake* pornografi di platform luar negeri (Reddit, X, Telegram, situs *deepfake* khusus).

Tindak pidana *deepfake* pornografi tidak hanya merupakan pelanggaran terhadap hukum, tetapi juga bentuk serangan serius terhadap martabat, hak privasi, dan integritas personal seseorang. Korban dari kejahatan ini mengalami berbagai dampak psikologis, sosial, dan hukum yang seringkali tidak tertangani dengan baik oleh sistem hukum yang ada. Perlindungan terhadap korban menjadi aspek penting yang harus diperhatikan secara komprehensif. Beberapa permasalahan utama dalam perlindungan korban antara lain:

1. Risiko Pencemaran Nama Baik dan Pelanggaran Privasi, *deepfake* pornografi pada umumnya menasar individu tertentu, sering kali tanpa sepengetahuan maupun persetujuan mereka. Wajah atau tubuh korban dimanipulasi dan disematkan ke dalam konten pornografi palsu, sehingga seolah-olah korban melakukan aktivitas seksual yang terekam dalam video tersebut. Akibatnya, korban

¹⁵ Wibowo, A., Wangsajaya, Y., & Surahmat, A. Pemolisian Digital dengan Artificial Intelligence. (PT. Raja Grafindo Persada Rajawali Pers, 2023)

¹⁶ Atem. “Ancaman Cyber Pornography Terhadap Anak-Anak”. *Jurnal Moral Kemasyarakatan* 1, No. 2 (2016): 113-114, doi: 10.21067/jmk.v1i2.1529.

mengalami kerusakan reputasi, gangguan mental, hingga stigma sosial yang berat. Selain itu, tindakan ini merupakan pelanggaran serius terhadap hak atas privasi yang dijamin dalam konstitusi maupun peraturan perundang-undangan.

2. Belum Adanya Mekanisme Pemulihan Khusus bagi Korban, sistem hukum di Indonesia belum memiliki mekanisme pemulihan yang dirancang secara khusus untuk korban kejahatan berbasis digital seperti *deepfake*. Tidak tersedia sistem bantuan hukum, pemulihan psikologis, atau layanan pemulihan nama baik yang terintegrasi. Lembaga-lembaga seperti LPSK (Lembaga Perlindungan Saksi dan Korban) umumnya fokus pada kejahatan konvensional, sehingga korban kejahatan digital acap kali merasa ditinggalkan atau tidak mendapatkan perlindungan yang layak. Hal ini menunjukkan adanya kekosongan perlindungan sekunder dan tersier terhadap korban kejahatan teknologi.

3. Upaya Hukum yang Dapat Dilakukan oleh Korban, meski perlindungan hukum belum maksimal, korban masih memiliki beberapa jalur upaya hukum yang dapat ditempuh. Di antaranya adalah:

- Melaporkan kasus ke Kepolisian, khususnya unit cyber crime.
- Menggunakan Pasal 27 ayat (1) dan Pasal 45 UU ITE untuk menuntut pelaku atas distribusi konten melanggar kesusilaan.
- Menempuh jalur perdata untuk menuntut ganti rugi atas kerugian yang ditimbulkan.
- Mengadukan kasus ke Komnas Perempuan, Kominfo, atau lembaga bantuan hukum. Namun, dalam praktiknya, banyak korban tidak melaporkan kasus karena ketidaktahuan, rasa takut, atau ketidakpercayaan pada efektivitas hukum.

Perkembangan teknologi informasi yang sangat cepat, khususnya kecerdasan buatan (*artificial intelligence/AI*), telah menciptakan bentuk-bentuk kejahatan baru yang belum sepenuhnya terakomodasi oleh regulasi yang ada. Salah satunya adalah kejahatan *deepfake* pornografi, yaitu konten pornografi hasil manipulasi AI yang dapat merusak reputasi seseorang tanpa melibatkan keterlibatan langsung korban. Keberadaan fenomena ini menunjukkan adanya kesenjangan antara hukum positif yang berlaku dengan realitas teknologi saat ini, sehingga diperlukan pembaruan regulasi secara

menyeluruh. Beberapa urgensi yang mendasari kebutuhan pembaruan tersebut antara lain:

1. Kebutuhan untuk Merevisi UU ITE agar Sesuai dengan Perkembangan Teknologi, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai dasar hukum dalam penanganan kejahatan digital di Indonesia, hingga saat ini belum secara eksplisit mengatur tentang teknologi manipulasi wajah (*deepfake*). Pasal-pasal yang digunakan, seperti Pasal 27 ayat (1) mengenai muatan melanggar kesusilaan, bersifat terlalu umum dan multitafsir. Akibatnya, proses penegakan hukum terhadap konten *deepfake* pornografi menjadi lemah secara normatif. Revisi terhadap UU ITE diperlukan untuk:

- Menambahkan pengaturan khusus mengenai penyalahgunaan teknologi berbasis AI.
- Memperjelas unsur pidana dalam konten hasil manipulasi digital.
- Memberikan kepastian hukum bagi aparat penegak hukum dan perlindungan maksimal bagi korban.

2. Gagasan Pembentukan Aturan Baru tentang Penyalahgunaan AI dan *Deepfake*. **Mengacu pada praktik hukum di beberapa negara maju, seperti Korea Selatan, Amerika Serikat, dan Inggris, telah terdapat aturan spesifik mengenai larangan pembuatan dan penyebaran *deepfake*, terutama dalam konteks pornografi dan fitnah. Hal ini dapat menjadi contoh bagi Indonesia untuk mulai menyusun regulasi baru yang lebih adaptif terhadap kemajuan teknologi, misalnya dalam bentuk:**

- Rancangan Undang-Undang (RUU) tentang Kecerdasan Buatan.
- Peraturan Pemerintah khusus mengenai manipulasi digital dan rekayasa visual.
- Sanksi pidana yang secara tegas menasar pembuat, penyebar, hingga platform penyedia konten *deepfake*.

Aturan baru ini tidak hanya dibutuhkan untuk mengisi kekosongan hukum, tetapi juga untuk memberikan efek jera, mengatur etika penggunaan AI, serta mencegah penyalahgunaan teknologi yang semakin masif.

Seiring pesatnya perkembangan teknologi digital, termasuk kecerdasan buatan (*artificial intelligence/AI*), tantangan hukum di masa depan akan semakin kompleks dan dinamis. Salah satu bentuk kejahatan modern yang perlu diantisipasi secara serius adalah *deepfake* pornografi, yang memiliki potensi tinggi untuk merusak reputasi,

privasi, dan kehormatan seseorang dalam hitungan detik. Oleh karena itu, diperlukan langkah konkret dalam membangun sistem hukum yang adaptif, preventif, dan responsif terhadap fenomena kejahatan digital berbasis teknologi.

PENUTUP

A. Kesimpulan

1. Pengaturan dalam Pasal 27 ayat (1) jo. Pasal 45 ayat (1) UU ITE memang mengandung larangan atas distribusi muatan yang melanggar kesusilaan, namun tidak secara eksplisit mengatur atau menyebut konten digital hasil manipulasi berbasis kecerdasan buatan seperti *deepfake*. Ketidakhadiran norma eksplisit tersebut menyebabkan hambatan dalam menjerat pelaku, terutama ketika pembuktian hukum bergantung pada identifikasi elemen fisik korban, niat jahat pelaku, dan autentisitas konten. *Deepfake* pornografi, yang pada dasarnya merupakan bentuk kekerasan seksual digital non-konsensual, menunjukkan celah dalam hukum positif Indonesia yang cenderung normatif dan tertinggal dari kemajuan teknologi. Selain itu, UU ITE belum membedakan antara pelaku pembuat, penyebar, maupun penyimpan konten, serta belum mengatur tanggung jawab korporasi digital atau platform yang memungkinkan konten tersebut beredar. Dalam praktiknya, penegakan hukum terhadap konten *deepfake* pornografi sering kali tidak berhasil karena pelaku menyembunyikan identitas melalui jaringan anonim atau beroperasi lintas negara, sementara aparat penegak hukum Indonesia masih memiliki keterbatasan dalam bidang digital forensik dan pelacakan identitas virtual. Oleh karena itu, diperlukan pembaruan hukum yang tidak hanya bersifat represif terhadap pelaku, tetapi juga preventif dan protektif terhadap korban, termasuk penambahan norma-norma baru yang mengatur secara spesifik kejahatan digital berbasis teknologi tinggi.
2. *Deepfake* pornografi bukan hanya kejahatan terhadap kesusilaan, melainkan juga merupakan bentuk pelanggaran serius terhadap hak atas privasi, martabat, dan integritas psikologis seseorang. Dalam konteks ini, sistem hukum pidana belum memiliki perangkat norma yang mampu memberikan perlindungan memadai bagi korban. Tidak adanya mekanisme pemulihan hukum yang terstruktur, baik secara administratif,

psikologis, maupun reputasional, menunjukkan bahwa perlindungan terhadap korban masih bersifat reaktif dan fragmentaris. Sementara itu, sanksi pidana dalam UU ITE yang tersedia pun tidak memberikan efek jera yang cukup kuat, mengingat kerusakan sosial dan pribadi akibat konten *deepfake* sering kali tidak sebanding dengan ancaman pidananya. Dalam menghadapi tantangan ini, negara harus mengambil peran sentral melalui pembentukan regulasi baru—seperti RUU tentang kecerdasan buatan, media digital, atau kekerasan seksual berbasis digital—yang secara khusus mengatur teknologi manipulatif seperti *deepfake*. Selain itu, perlu dilakukan pelatihan teknis bagi aparat penegak hukum, pengembangan laboratorium digital forensik yang modern, serta peningkatan kerja sama internasional untuk menanggulangi kejahatan lintas negara. Tak kalah penting, pemerintah juga harus mendorong tanggung jawab platform digital dalam mendeteksi, menghapus, dan mencegah penyebaran konten ilegal, sekaligus mengedukasi masyarakat tentang literasi digital dan etika penggunaan teknologi. Penanganan terhadap kejahatan *deepfake* pornografi tidak hanya menuntut kekuatan hukum, tetapi juga strategi nasional yang inklusif dan berbasis pada prinsip keadilan digital dan perlindungan hak asasi manusia di era teknologi 5.0.

B. Saran

1. Salah satu hal mendesak yang harus dilakukan pemerintah Indonesia adalah merevisi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta menyusun regulasi khusus yang secara tegas dan eksplisit mengatur tindak pidana yang berasal dari penyalahgunaan teknologi kecerdasan buatan, seperti *deepfake* pornografi. UU ITE saat ini masih terlalu umum dan belum mampu mengakomodasi karakteristik baru dari konten manipulatif digital yang dihasilkan oleh AI. Pemerintah perlu mempertimbangkan pembentukan Undang-Undang baru atau menambahkan ketentuan dalam UU ITE yang mengatur secara khusus tentang kejahatan berbasis AI, termasuk pembuat, penyebar, penyimpan, dan penyedia platform. Selain itu, perlunya aturan tentang pertanggungjawaban pidana korporasi dan penyedia teknologi, termasuk batasan etis dalam pengembangan dan penggunaan AI, sangat penting untuk

menutup celah hukum yang selama ini dimanfaatkan oleh pelaku kejahatan digital.

2. Dalam menghadapi kejahatan digital yang semakin kompleks, dibutuhkan peningkatan kualitas sumber daya manusia di bidang penegakan hukum, khususnya penyidik, jaksa, dan hakim, agar mampu memahami, mendeteksi, dan membuktikan tindak pidana yang berbasis teknologi AI seperti *deepfake*. Pelatihan khusus dalam bidang digital forensik, investigasi siber, dan hukum siber menjadi keharusan agar aparat dapat bertindak cepat dan tepat. Selain itu, pemerintah juga perlu melibatkan masyarakat secara aktif melalui kampanye edukasi dan literasi digital untuk meningkatkan kesadaran hukum masyarakat mengenai bahaya dan dampak dari konten *deepfake* pornografi. Peran media, lembaga pendidikan, dan organisasi masyarakat sipil menjadi penting dalam menyampaikan informasi yang benar, serta mendorong korban untuk berani melapor dan mendapatkan perlindungan yang layak.

DAFTAR PUSTAKA

Buku :

- Ali, A. (2022). *Menguak tabir hukum: Suatu kajian filosofis dan sosiologis*. Jakarta: PT Toko Gunung Agung.
- Lamintang, P. A. F. (2014). *Dasar-dasar hukum pidana di Indonesia*. Jakarta: Sinar Grafika.
- Lesmana, T. (1995). *Pornografi dalam media massa*. Jakarta: Puspa Swara.
- Marr, B. (2020). *The intelligence revolution: Transforming your business with AI*. New York: Kogan Page.
- Maskun. (2011). *Pengantar cybercrime*. Makassar: Pustaka Pena Press.
- Mubarok, N., & Hajar, I. I. (2020). *Buku ajar hukum pidana* (Edisi pertama). Sidoarjo: Kanzun Books.
- Prodjodikoro, W. (2003). *Tindak pidana tertentu di Indonesia*. Bandung: PT Rafika Aditama.
- Putra, I. H. (2023). Perlindungan hukum terhadap korban penyalahgunaan artificial intelligence (AI) berupa *deepfake* pornografi menurut peraturan perundang-undangan. *UNJA Journal of Legal Studies*, 1(2), 114–123.
- Raharjo, S. (2004). Reformasi menuju hukum progresif. *Unisia*, 27(53), 238–241.
- Rahardjo, S. (2009). *Hukum progresif*. Yogyakarta: Genta Press.
- Raharjo, A. (2002). *Cyber crime: Pemahaman dan upaya pencegahan kejahatan berteknologi*. Bandung: Citra Aditya Bakti.
- Renata. (2022). *Aspek hukum perlindungan data pribadi source subject terhadap penggunaan teknik deepfake dalam perspektif perbuatan melanggar hukum*. Indralaya: Fakultas Hukum Universitas Sriwijaya.
- Sandra, R., Sepriano, & Sudipa, I. (2023). *Fenomena artificial intelligence (AI)* (Edisi 1). Jambi: PT Sonpedia Publishing Indonesia.
- Schaffmeistr, Kejizer, & Sutorius. (2007). *Hukum pidana*. Bandung: Citra Aditya Bakti.
- Sofyan, A. (2016). *Buku ajar hukum pidana*. Makassar: Pustaka Pena Pers.
- Van Bemmelen, J. M. (1986). *Hukum pidana III: Bagian khusus delik-delik khusus*. Jakarta: Bina Cipta.
- Wibowo, A., Wangsajaya, Y., & Surahmat, A. (2023). *Pemolisian digital dengan artificial intelligence*. Jakarta: PT Raja Grafindo Persada Rajawali Pers.
- ##### Jurnal :
- Amelia, Y. F., Kaimuddin, A., & Ashsyarofi, H. L. (2023). Pertanggungjawaban pidana pelaku terhadap korban penyalahgunaan artificial intelligence *deepfake* menurut hukum positif Indonesia. *Dinamika*, 30(1), 96–110.
- Atem. (2016). Ancaman cyber pornography terhadap anak-anak. *Jurnal Moral Kemasyarakatan*, 1(2), 113–114. <https://doi.org/10.21067/jmk.v1i2.1529>
- Aulia, M. Z. (2018). Ulasan tokoh dan pemikiran hukum hukum progresif dari Satjipto Rahardjo: Riwayat, urgensi, dan relevansi. *Undang: Jurnal Hukum*, 1(1), 159–185.
- Hafsyari, Z. S., dkk. (2023). Korban *deepfake* pornografi: Evaluasi efektivitas hukum positif dan kebutuhan akan reformasi hukum. *Medium*. <https://pleads-fhunpad.medium.com/perindungan-hukum-bagi-korban-deepfake-pornografi-evaluasi-efektivitas-hukum-positif-dan-1fb2bb20da35> (Diakses 15 April 2025)
- Jufri, & Putra. (2022). Aspek hukum internasional dalam pemanfaatan *deepfake* technology terhadap perlindungan data pribadi. [Nama Jurnal Belum Tersedia], 1(1), 36–45. (Perlu dilengkapi nama jurnal dan volume jika tersedia.)
- Khusna, I. H., & Pangestu, S. (2019). *Deepfake*, tantangan baru untuk netizen. *Jurnal Promedia*, 5(2), 1–8.
- Luh Putu. (2021). Peran artificial intelligence (AI) untuk mendukung pembelajaran di masa pandemi COVID-19. *Jurnal Komputer dan Teknologi Sains (KOMTEKS)*, 1, 15–23.

- Putra, I. H. (2023). Perlindungan hukum terhadap korban penyalahgunaan artificial intelligence (AI) berupa *deepfake* pornografi menurut peraturan perundang-undangan. *UNJA Journal of Legal Studies*, 1(2), 114–123.
- Samin, H. H. (2023). Perlindungan hukum terhadap kebocoran data pribadi oleh pengendali data melalui pendekatan hukum progresif. *Ampus Akademik Publishing Jurnal Sains Student Research*, 1(2).
- Tan, D. (2021). Metode penelitian hukum: Mengupas dan mengulas metodologi dalam menyelenggarakan penelitian hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, 8(8), 2463–2478.
- Utama, A. N., Kesuma, P. T., & Hidayat, R. M. (2023). Analisis hukum terhadap upaya pencegahan kasus *deepfake* porn dan pendidikan kesadaran publik di lingkungan digital. *Jurnal Pendidikan Tambusai*, 7(3), 26179–26188.
- Utawi, E. I., & Ruhaeni, N. (2023). Penegakan hukum terhadap tindak pidana pornografi menurut peraturan perundang-undangan tentang pornografi melalui media sosial. *Bandung Conference Series: Law Studies*, 3(1), 365.
- Valerian, D. (2022). Kriteria kriminalisasi: Analisis pemikiran Moeljatno, Sudarto, Theo De Roos, dan Iris Haenen. *Jurnal Veritas Et Justitia*, 8(2), 422–423. <https://doi.org/10.25123/vej.v8i2.4923>
- Department. Diakses dari <http://jmc.stanford.edu/articles/whatisai/whatisai.pdf>
- Tangerangnews.com. (2024, November 6). AI makin ngeri, ini cara membuat video *deepfake*. Diakses dari <https://www.tangerangnews.com/tekno/read/48964/AI-Makin-Ngeri-Ini-Cara-Membuat-Video-Deepfake>
- Universitas Muhammadiyah Yogyakarta. (2024, Agustus 6). Pendekatan yuridis normatif adalah pendekatan yang dilakukan berdasarkan bahan hukum. Diakses dari <https://repository.umy.ac.id/bitstream/handle/123456789/28995/bab%203.pdf?seque#:~:text=Pendekatan%20yuridis%20normatif%20adalah%20pendekatan%20yang%20dilakukan%20berdasarkan%20bahan%20hukum,yang%20berhubungan%20dengan%20penelitian%20ini>
- Universitas Indonesia. (2024, September 12). Faktor-faktor yang berhubungan dengan penelitian ini. Diakses dari <https://lib.ui.ac.id/file?file=digital/old8/123423-S-5540-Faktor-faktor%20yang-Literatur.pdf>
- Wikipedia. (2025). Pornografi. Diakses dari <https://id.wikipedia.org/wiki/Pornografi>

Peraturan perundang-undangan:

- Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).
- Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang Pornografi.

Internet :

- Hukumonline. (2024, Agustus 4). Apa itu *deepfake* porn dan jerat pidana bagi pelakunya. Diakses dari https://www.hukumonline.com/klinik/a/apa-itu-deepfake-porn-dan-jerat-pidana-bagi-pelakunya-lt6530d3546d9c4/#_ftn13
- Hybrid.co.id. (2024, Agustus 24). *Deepfake*: Definisi dan contoh penggunaan agar Anda bisa waspada. Diakses dari <https://hybrid.co.id/post/deepfake-definisi-dan-contoh-penggunaan-agar-anda-bisa-waspada/>
- John McCarthy. (2004, November). What is Artificial Intelligence? Computer Science