

Deepfake Dan Krisis Kepercayaan: Analisis Hukum Terhadap Penyebaran Konten Palsu Di Media Sosial

Deepfakes and the Crisis of Trust: A Legal Analysis of the Spread of Fake Content on Social Media

Dwi Fitri¹, Ade Nur Hidayah², Aulia Putri³, Nazwa Hanifah Tanjung⁴, Sania Izzati Ramadhani⁵, Dara Akila⁶, Rezita Ardhani Manurung⁷, Nawal Mufidah⁸, Syakban Akbar⁹, Muhammad Zikri¹⁰

Universitas Malikussaleh

Email: dwifitri@unimal.ac.id, nzwtanjung709@gmail.com

Article Info

Article history :

Received : 01-06-2025

Revised : 03-06-2025

Accepted : 05-06-2025

Published : 07-06-2025

Abstract

The advancement of digital technology, particularly artificial intelligence (AI), has led to the emergence of deepfake—a technique that enables realistic manipulation of audio, video, images, and text. Although initially developed for entertainment and research, its misuse has sparked serious issues such as disinformation, financial fraud, personal harassment, and a growing public distrust in digital media. This article explores the social and legal impacts of deepfake content on social media, as well as the effectiveness of Indonesian regulations in addressing these challenges. Using a qualitative approach and literature study method, the article highlights the urgency of legal reform, the importance of digital literacy, and the need for cross-sector collaboration to mitigate the risks posed by deepfake technology.

Keywords: Deepfake, Artificial Intelligence, Disinformation

Abstrak

Kemajuan teknologi digital, khususnya kecerdasan buatan (AI), telah melahirkan fenomena *deepfake* yang memungkinkan manipulasi audio, video, gambar, dan teks secara realistis. Meskipun awalnya dikembangkan untuk hiburan dan riset, penyalahgunaan teknologi ini menimbulkan berbagai permasalahan, mulai dari penyebaran disinformasi, penipuan finansial, pelecehan personal, hingga krisis kepercayaan publik terhadap media digital. Artikel ini membahas dampak sosial dan hukum dari penyebaran konten *deepfake* di media sosial serta efektivitas regulasi hukum di Indonesia dalam menanggulangnya. Menggunakan pendekatan kualitatif dengan metode studi literatur, artikel ini mengungkap urgensi pembaruan hukum, pentingnya literasi digital, serta perlunya kolaborasi lintas sektor untuk menghadapi tantangan yang ditimbulkan oleh teknologi *deepfake*.

Kata Kunci: Deepfake, Kecerdasan Buatan, Disinformasi

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di Indonesia berlangsung dengan sangat pesat. Dari waktu ke waktu, kemajuan teknologi informasi telah membawa perubahan yang cepat dan signifikan dalam kehidupan kita tanpa batas. Kehadiran teknologi ini memberikan banyak manfaat bagi kesejahteraan dan kemajuan, memfasilitasi penyebaran informasi dan pengetahuan dari seluruh dunia yang melintasi batas ruang dan waktu. Namun, di samping itu, terdapat juga dampak negatif yang muncul. Peningkatan kejahatan dengan berbagai modus operandi memanfaatkan teknologi dan informasi telah mengakibatkan perubahan nilai, moral,

dan norma yang seringkali bertentangan dengan kehidupan masyarakat.

Salah satu bentuk pelanggaran hukum yang semakin marak terjadi di dunia maya adalah kejahatan siber. Kejahatan ini, yang dikenal dengan istilah Cyber Crime, merupakan salah satu manifestasi baru dari kriminalitas di era modern yang didasarkan pada kecanggihan teknologi. Kejahatan siber bersifat universal dan multidimensional dalam lingkup dunia maya, serta memiliki dampak negatif yang nyata dalam kehidupan manusia sehari-hari. Kejahatan siber ini sering kali digunakan sebagai alat untuk pelecehan seksual, penyebaran berita hoaks, dan tindak pidana pornografi. Fenomena kejahatan siber telah menjadi ancaman bagi stabilitas keamanan, sehingga pemerintah menghadapi kesulitan dalam mengimbangi teknik-teknik kriminal yang dilakukan dengan teknologi komputer. Tindak pidana pornografi merupakan salah satu contoh kejahatan siber yang saat ini paling banyak terjadi di Indonesia.

Perkembangan teknologi, baik di dunia maupun di Indonesia, semakin pesat. Salah satu contohnya adalah kecerdasan buatan atau artificial intelligence (AI), yang merupakan tonggak kemajuan teknologi di era digital. AI memberikan dampak positif di berbagai aspek kehidupan. Kini, teknologi tidak hanya bergantung pada kecerdasan manusia, tetapi juga memiliki kemampuan cerdasnya sendiri. AI merupakan bagian dari sistem pengolahan berbasis komputer yang mampu mempelajari dan melaksanakan tugas-tugas dengan cara yang mirip atau bahkan lebih baik dibandingkan manusia. Di tengah masyarakat, artificial intelligence memiliki pengaruh yang signifikan. Namun, sayangnya, teknologi ini juga sering disalahgunakan oleh penjahat siber dalam praktik yang dikenal sebagai Artificial Intelligence-Crime (AIC). Salah satu hasil dari penerapan teknologi ini adalah Deepfake, yang perlu diwaspadai dalam konteks keamanan dan etika. Dalam tangan yang salah, teknologi ini dapat disalahgunakan untuk tujuan yang merugikan, seperti menciptakan konten palsu (deepfake) yang dapat merusak reputasi individu atau bahkan memicu kekacauan sosial. (Natanael,dkk 2025).

Analisis yuridis mengenai penggunaan AI dalam kejahatan siber harus memperhatikan peran serta tanggung jawab dari semua pihak yang terlibat. Tidak hanya pelaku tindak kejahatan yang perlu dimintai pertanggungjawaban, tetapi juga para pengembang teknologi dan penyedia layanan digital yang memberikan ruang bagi terjadinya pelanggaran. Isu mengenai siapakah yang bertanggung jawab jika AI melakukan kesalahan atau dimanfaatkan untuk melakukan kejahatan menjadi penting dan perlu dibahas secara mendalam. Peran pemerintah dan lembaga internasional dalam mengatur serta mengawasi penggunaan AI juga sangat vital. Di era globalisasi ini, kejahatan siber sering kali melibatkan berbagai yurisdiksi, sehingga memerlukan kerjasama internasional yang solid untuk menanggulangi permasalahan tersebut. Pemerintah harus merumuskan kebijakan yang tepat untuk menjamin penggunaan AI yang baik, baik dalam konteks penegakan hukum maupun pencegahan kejahatan siber. Pada saat bersamaan, kerjasama internasional harus diperkuat agar penegakan hukum dapat dilaksanakan secara efektif di seluruh dunia.

Di Indonesia sendiri, penerapan AI dalam penegakan hukum masih berada pada tahap awal. Meskipun pemerintah telah mengakui pentingnya teknologi AI dalam menghadapi ancaman kejahatan siber, implementasinya masih terbatas dan regulasinya belum sepenuhnya siap menghadapi berbagai tantangan yang ada. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang menjadi dasar hukum penanganan kejahatan siber perlu ditinjau

kembali dan disesuaikan dengan perkembangan teknologi, termasuk AI. Pendekatan yuridis dalam menangani penggunaan AI dalam kejahatan siber juga harus melibatkan berbagai disiplin ilmu, seperti ilmu komputer, etika, dan kriminologi.

Seiring dengan meningkatnya penggunaan deepfake, usaha untuk mendeteksi dan menangani dampaknya semakin berkembang. Berbagai metode deteksi deepfake telah dirancang, termasuk teknik pembelajaran dalam dan pembelajaran mesin yang bertujuan untuk mengenali manipulasi wajah dalam video dan gambar. Selain itu, peningkatan literasi digital dan kesadaran masyarakat mengenai bahaya deepfake menjadi sangat penting untuk menghadapi disinformasi yang ditimbulkan oleh konten sintesis. Melalui kolaborasi antara teknologi, regulasi, dan pendidikan, diharapkan ancaman yang ditimbulkan oleh deepfake dapat diminimalisir, sehingga menjaga integritas informasi di era digital.

Analisis yuridis terkait penggunaan AI dalam kejahatan siber harus mampu mengidentifikasi potensi risiko, menawarkan solusi yang efektif, dan memastikan hukum dapat berfungsi dengan baik menghadapi tantangan yang ada. Untuk mencapai tujuan ini, diperlukan upaya berkelanjutan dari berbagai pihak, termasuk pemerintah, aparat penegak hukum, pengembang teknologi, dan masyarakat luas. Hanya dengan kerjasama yang baik dan regulasi yang tepat, kita dapat memastikan bahwa perkembangan teknologi, termasuk AI, digunakan untuk kebaikan, bukan disalahgunakan untuk tujuan yang merugikan. Sebagai negara yang sedang berkembang, Indonesia perlu terus memperkuat regulasi dan infrastruktur hukumnya agar dapat mengikuti perkembangan teknologi dan bersiap menghadapi tantangan kejahatan siber di masa mendatang.

METODOLOGI PENELITIAN

Penelitian ini dikategorikan sebagai penelitian kualitatif, yaitu suatu pendekatan ilmiah yang menekankan pada pemahaman mendalam terhadap suatu fenomena sosial, budaya, atau perilaku manusia berdasarkan perspektif subjek yang diteliti. Dalam konteks ini, data yang dikumpulkan tidak bersifat numerik, melainkan berupa narasi, deskripsi, atau dokumen yang diambil dari berbagai sumber, seperti literatur jurnal ilmiah, serta studi literatur lainnya yang relevan. Pendekatan kualitatif bertujuan untuk menggali makna, pola, serta hubungan antar fenomena yang kompleks dan tidak dapat diukur secara kuantitatif. Oleh karena itu, proses observasi dalam penelitian kualitatif dilakukan secara mendalam dan berkelanjutan, guna memperoleh pemahaman yang lebih tajam terhadap konteks serta latar belakang permasalahan yang sedang dikaji. Dengan menggunakan metode ini, peneliti dapat mengidentifikasi akar permasalahan, menginterpretasikan makna-makna yang terkandung dalam perilaku atau kejadian, serta menyusun rumusan masalah secara komprehensif dan kontekstual.

HASIL DAN PEMBAHASAN

1. Pengertian Deepfake

Deepfake adalah teknologi manipulasi video dan audio yang memanfaatkan kecerdasan buatan (AI) untuk menciptakan konten yang tampak atau terdengar nyata, padahal sebenarnya palsu. Muncul sejak 2017, teknologi ini terus berkembang, menghasilkan video dan audio yang semakin sulit dibedakan dari yang asli. Kemampuannya untuk mengganti wajah dan suara seseorang dalam video telah menimbulkan kekhawatiran

serius terkait keamanan dan privasi, mengingat potensi penyalahgunaannya untuk menyebarkan informasi palsu atau merusak reputasi. Memahami cara kerja deepfake dan implikasinya sangat krusial dalam menghadapi tantangan dunia digital saat ini. (Amalia, dkk 2022).

Istilah deepfake berasal dari kombinasi dua kata yang terkait dengan metode memanipulasi konten visual dan audio dalam algoritma pembelajaran yang mendalam. Menggunakan teknologi ini, orang dapat mengubah representasi tubuh seseorang dengan akurasi yang sangat tinggi dalam video dan gambar, membuatnya sulit untuk membedakannya dari konten asli. Deepfake menggunakan jaringan saraf buatan, khususnya jaringan generatif dan kontroversial (Goose) untuk menciptakan media sintesis otentik. Pertama-tama teknologi ini dikembangkan untuk tujuan hiburan dan untuk penelitian ilmiah. Namun pada kenyataannya, deepfake digunakan untuk tujuan berbahaya seperti

Deepfake memanfaatkan algoritma deep learning untuk meniru wajah seseorang dengan sangat akurat, mencakup berbagai sudut pandang dan ekspresi. Dua metode utama digunakan: Deep Neural Networks (DNN) dan Generative Adversarial Networks (GANs). DNN, sebuah jaringan saraf tiruan yang kompleks, dilatih untuk mereplikasi ekspresi wajah, gerakan bibir, dan gerakan mata. Proses pelatihan ini membutuhkan data yang sangat banyak dan waktu yang lama. Sementara itu, GANs menggunakan dua jaringan saraf yang saling bersaing: sebuah generator yang menciptakan deepfake, dan sebuah discriminator yang berusaha membedakan antara deepfake dan video asli. Persaingan ini menghasilkan deepfake yang semakin realistis.

Meskipun kemampuan deepfake menghadirkan potensi positif di bidang hiburan dan efek visual, dampak negatifnya jauh lebih mengkhawatirkan. Kemudahan pembuatan deepfake meningkatkan risiko penyebaran informasi palsu, manipulasi opini publik, dan kerusakan reputasi individu. Oleh karena itu, peningkatan kesadaran publik, pengembangan metode deteksi yang efektif, dan regulasi yang tepat sangat penting untuk mengurangi dampak negatif deepfake.

Seiring perkembangan teknologi, kecerdasan buatan (AI) telah diterapkan dalam berbagai bidang, mulai dari bisnis hingga hiburan. Salah satu bentuk evolusi teknologi ini adalah deepfake, yang menggabungkan deep learning dan konten palsu. Teknologi ini menggunakan jaringan saraf tiruan untuk menciptakan gambar atau video yang sangat realistis namun palsu. Pada dasarnya, deepfake bekerja dengan dua algoritma utama: generator yang menciptakan konten, dan discriminator yang memverifikasi keasliannya. Kedua algoritma ini terus berinteraksi, meningkatkan kemampuan mereka untuk menghasilkan konten yang hampir tidak bisa dibedakan dari yang asli. Awalnya, deepfake lebih sering digunakan dalam dunia hiburan atau sebagai guyonan semata. Namun, seiring berjalannya waktu, teknologi ini mulai digunakan untuk tujuan yang lebih serius dan bahkan berbahaya. Sebagai contoh, deepfake kini dapat digunakan untuk menyebarkan informasi palsu, merusak reputasi seseorang, atau bahkan untuk balas dendam. Hal ini menjadi semakin mengkhawatirkan, mengingat siapa saja yang memiliki jejak digital di media sosial bisa menjadi sasaran. (Rendy Pabalbesy, 2019).

Proses pembuatan deepfake sendiri cukup sederhana; dengan menyediakan ratusan hingga ribuan foto atau video seseorang, AI akan secara otomatis mengganti wajah orang tersebut dengan wajah orang lain. Semakin banyak data yang disediakan, semakin realistis hasilnya. Ini berarti, platform media sosial seperti Instagram, Twitter, dan YouTube menjadi sumber utama untuk mengumpulkan data bagi pembuatan deepfake. Teknologi ini menggunakan metode Generative Adversarial Network (GAN), di mana AI terus-menerus belajar dan memperbaiki diri untuk menghasilkan video yang tampak asli. Yang lebih mencemaskan lagi, saat ini pembuatan deepfake tidak memerlukan keahlian khusus, karena

banyak tutorial gratis di internet. Ke depannya, kita akan semakin kesulitan membedakan video asli dari yang palsu.

2. Dampak Sosial dari Deepfake

Teknologi deepfake, yang memungkinkan pembuatan konten audio dan visual yang sangat realistis dengan meniru suara atau wajah seseorang, membawa dampak sosial yang signifikan, terutama dalam dunia kejahatan siber dan kepercayaan terhadap informasi digital. Salah satu dampak paling mengkhawatirkan dari teknologi ini adalah kemampuannya untuk digunakan dalam penipuan finansial. Dengan kemampuan untuk meniru suara eksekutif atau individu lain secara sangat meyakinkan, para pelaku kejahatan siber dapat memanipulasi korban untuk melakukan tindakan yang merugikan. Sebagai contoh, ada laporan internasional tentang kasus di mana deepfake digunakan untuk menipu manajer keuangan dalam perusahaan agar mentransfer sejumlah besar dana ke rekening yang dikendalikan oleh penipu. Tidak hanya menyebabkan kerugian finansial yang besar, tetapi juga memberikan dampak negatif yang lebih luas, yaitu merusak reputasi dan kredibilitas perusahaan yang menjadi korban penipuan tersebut.

Kejahatan semacam ini memperlihatkan betapa seriusnya ancaman yang ditimbulkan oleh teknologi deepfake, terutama di sektor-sektor yang sangat bergantung pada keamanan informasi dan transaksi finansial. Dalam konteks ini, dibutuhkan upaya mitigasi yang lebih sistematis untuk meminimalisir dampak dari teknologi ini. Salah satu langkah penting adalah memberikan pelatihan keamanan siber yang lebih intensif kepada para karyawan, khususnya di sektor-sektor yang rawan terhadap ancaman semacam ini. Selain itu, meningkatkan kesadaran mengenai potensi risiko yang ditimbulkan oleh deepfake serta memperkuat protokol dan sistem keamanan yang ada akan menjadi hal yang sangat penting dalam menghadapi ancaman yang terus berkembang ini. penyebaran konten deepfake di media sosial berkontribusi pada memburuknya krisis kepercayaan terhadap informasi yang beredar di dunia maya. Banyak pengguna media sosial kini merasa semakin kesulitan untuk membedakan antara konten yang asli dan yang telah dimanipulasi, yang pada gilirannya menurunkan tingkat kepercayaan publik terhadap sumber informasi digital. Hal ini juga menyebabkan munculnya skeptisisme yang lebih besar terhadap berita yang dibagikan di media sosial, mengingat kenyataan bahwa deepfake dapat dengan mudah membuat informasi yang salah tampak sangat meyakinkan dan sulit dibedakan dari kebenaran.

Dalam banyak kasus, konten deepfake yang sensasional atau provokatif lebih cenderung untuk menjadi viral, berkat algoritma platform yang memprioritaskan jenis konten ini karena potensi jangkauannya yang besar. Fenomena ini bukan hanya merusak hubungan

antara masyarakat dan media digital, tetapi juga mengurangi efektivitas media sosial sebagai alat komunikasi dan sumber informasi yang dapat dipercaya. Sebagai respons terhadap hal ini, kolaborasi antara berbagai pihak, termasuk platform teknologi, pemerintah, dan komunitas akademik, menjadi sangat penting. Upaya bersama ini dapat membantu mengembangkan sistem deteksi deepfake yang lebih efisien serta meningkatkan transparansi dalam pengelolaan konten di media sosial. Dengan adanya teknologi deteksi yang lebih baik, diharapkan kita dapat mengurangi dampak negatif dari penyebaran konten palsu dan kembali membangun kepercayaan masyarakat terhadap media digital.

Secara keseluruhan, meskipun teknologi deepfake memiliki potensi untuk digunakan dalam berbagai bidang yang bermanfaat, dampak sosial dan keamanannya tidak dapat diabaikan begitu saja. Diperlukan langkah-langkah proaktif dalam menghadapi ancaman ini, baik di tingkat individu, perusahaan, maupun negara, guna memastikan bahwa teknologi ini tidak disalahgunakan dan tidak merusak tatanan sosial yang telah ada.

3. Jenis Konten *Deepfake*

Deepfake merupakan sebuah inovasi di bidang teknologi digital yang melibatkan penggunaan kecerdasan buatan untuk merekayasa berbagai bentuk konten. Di Indonesia, fenomena ini mulai menjadi perhatian serius seiring dengan maraknya penyalahgunaan teknologi untuk disinformasi dan manipulasi opini publik. Secara umum, konten deepfake dapat dibedakan menjadi beberapa kategori utama: video, audio, gambar, teks, dan kombinasi multimodal, yang masing-masing memiliki karakteristik khusus serta tantangan tersendiri (Hendrawan, 2021).

a. Deepfake Video

Deepfake video adalah bentuk paling dikenal, di mana wajah atau ekspresi seseorang diubah dalam video untuk membuatnya tampak melakukan atau mengatakan sesuatu yang sebenarnya tidak terjadi. Di Indonesia, fenomena ini telah digunakan untuk menyebarkan disinformasi, terutama dalam konteks politik dan sosial. Misalnya, video yang dimanipulasi untuk menampilkan tokoh publik melakukan tindakan yang kontroversial dapat mempengaruhi opini publik dan menciptakan ketegangan sosial.

b. Deepfake Audio

Deepfake audio melibatkan peniruan suara seseorang untuk membuat rekaman palsu yang terdengar autentik. Teknologi ini memungkinkan pembuatan rekaman suara yang menyerupai tokoh publik, yang kemudian dapat digunakan untuk menyebarkan informasi palsu atau melakukan penipuan. Di Indonesia, penggunaan deepfake audio telah menimbulkan kekhawatiran terkait penyebaran hoaks dan manipulasi informasi.

c. Deepfake Gambar

Manipulasi gambar menggunakan teknologi deepfake memungkinkan penciptaan foto-foto yang tampak nyata namun sebenarnya palsu. Gambar-gambar ini dapat digunakan untuk berbagai tujuan, termasuk pencemaran nama baik, penipuan identitas, dan penyebaran konten pornografi tanpa persetujuan individu yang bersangkutan. Kasus-kasus seperti ini telah terjadi di Indonesia, menimbulkan kekhawatiran tentang privasi dan

perlindungan data pribadi .

d. Deepfake Teks

Meskipun kurang umum, deepfake teks melibatkan penggunaan AI untuk meniru gaya penulisan seseorang, menghasilkan dokumen atau pesan yang tampak ditulis oleh individu tertentu. Teknologi ini dapat digunakan untuk menyebarkan informasi palsu atau melakukan penipuan melalui komunikasi tertulis. Di Indonesia, potensi penyalahgunaan deepfake teks masih menjadi area yang memerlukan perhatian lebih lanjut.

e. Konten Multimodal

Konten multimodal menggabungkan berbagai bentuk deepfake—video, audio, dan teks— untuk menciptakan konten yang sangat meyakinkan dan sulit dibedakan dari yang asli. Penggunaan konten multimodal ini dapat memperkuat efek manipulatif, meningkatkan risiko penyebaran disinformasi, dan menantang upaya deteksi serta penanggulangan. Di Indonesia, perkembangan konten multimodal deepfake menjadi perhatian serius dalam konteks keamanan informasi dan perlindungan masyarakat

4. Tinjauan Hukum Terkait *Deepfake* di Indonesia

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 DeepfakePorn, 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, kesadaran 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.

Sampai saat ini, Indonesia belum memiliki kerangka hukum yang secara spesifik dan komprehensif mengatur penggunaan kecerdasan buatan (AI). Meskipun unsur AI telah disebut dalam Undang-Undang Nomor 1 Tahun 2004 yang merupakan perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), regulasi tersebut hanya sebatas mengakui AI sebagai agen elektronik, yaitu perangkat yang mampu menjalankan tindakan otomatis berdasarkan data atau informasi elektronik .

Namun, aturan ini belum menyentuh aspek-aspek krusial seperti etika penggunaan AI, (Mperlindungan privasi, dan dampak sosial yang ditimbulkan oleh teknologi tersebut. Ketiadaan regulasi khusus ini menimbulkan ketidakjelasan mengenai tanggung jawab hukum, standar etis, dan risiko sosial yang terkait dengan pemanfaatan AI di berbagai sektor.

5. Dampak Penyebaran Konten Deepfake terhadap kepercayaan Publik

Perkembangan kecerdasan buatan (artificial intelligence) telah melahirkan berbagai inovasi, salah satunya teknologi deepfake. Teknologi ini memungkinkan manipulasi media digital terutama video dan audio dengan hasil yang sangat realistis sehingga sulit dibedakan dari konten asli. Meskipun awalnya dimanfaatkan dalam industri hiburan dan pendidikan, penyalahgunaan deepfake telah menciptakan persoalan serius di masyarakat, khususnya terkait penyebaran disinformasi dan erosi kepercayaan publik (Fadillah & Setiawan, 2022).

Dalam konteks sosial, deepfake telah banyak digunakan untuk melecehkan individu, terutama perempuan, melalui pembuatan konten eksplisit yang merusak reputasi serta menimbulkan trauma psikologis. Penelitian menunjukkan bahwa 47% dari kasus

penyalahgunaan deepfake yang dianalisis berkaitan dengan pelecehan personal. Kondisi ini diperburuk oleh minimnya perlindungan hukum bagi korban serta keterbatasan regulasi yang ada (Fadillah & Setiawan, 2022). Sementara itu, dalam ranah politik, konten deepfake telah digunakan sebagai alat propaganda untuk menyebarkan narasi palsu yang dapat menggiring opini publik. Menjelang pemilihan umum, misalnya, muncul berbagai video manipulatif yang menampilkan tokoh politik mengucapkan pernyataan kontroversial yang sebenarnya tidak pernah mereka katakan. Sekitar 32% dari kasus yang diteliti berkaitan dengan disinformasi politik. Fenomena ini menunjukkan bahwa deepfake bukan hanya menyerang individu, tetapi juga dapat mengancam stabilitas politik dan integritas demokrasi (Fadillah & Setiawan, 2022; Kurniawan & Mustikasari, 2020). Krisis kepercayaan terhadap media sosial pun semakin dalam. Banyak pengguna kesulitan membedakan antara konten asli dan palsu karena kualitas visual deepfake yang sangat meyakinkan. Seperti dikemukakan oleh Fadillah dan Setiawan (2022), “banyak pengguna media sosial tidak menyadari bagaimana mengenali konten deepfake, yang sering kali terlihat sangat meyakinkan” (hlm. 3). Kondisi ini diperburuk oleh algoritma media sosial yang cenderung mempromosikan konten sensasional, termasuk deepfake, demi keterlibatan pengguna.

Selain itu, dimensi ekonomi juga terdampak oleh penyalahgunaan teknologi ini. Deepfake audio telah digunakan untuk menipu pihak perusahaan dengan meniru suara eksekutif agar melakukan transaksi finansial ilegal. Sekitar 21% dari penyalahgunaan deepfake berkaitan dengan penipuan semacam ini. Kejahatan tersebut tidak hanya menimbulkan kerugian finansial, tetapi juga merusak reputasi perusahaan yang menjadi korban (Juefei-Xu et al., 2022).

Sayangnya, Indonesia belum memiliki regulasi khusus yang dapat secara efektif menangani kasus-kasus penyalahgunaan teknologi ini. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan UU Perlindungan Data Pribadi (UU PDP) belum dirancang untuk mengakomodasi kompleksitas teknologi deepfake. Sebagai pembanding, Uni Eropa melalui Artificial Intelligence Act telah lebih progresif dalam menyusun kerangka hukum yang adaptif terhadap teknologi baru (Fadillah & Setiawan, 2022). Untuk mengatasi tantangan ini, diperlukan pendekatan sistemik yang melibatkan pembentukan regulasi hukum yang spesifik, peningkatan literasi digital masyarakat, dan pengembangan teknologi pendeteksi deepfake yang lebih akurat. Kolaborasi antara pemerintah, perusahaan teknologi, dan

komunitas akademik juga menjadi kunci dalam menciptakan ekosistem digital yang lebih bertanggung jawab dan transparan. Harapannya, masyarakat dapat lebih siap menghadapi dampak teknologi digital tanpa kehilangan kepercayaan terhadap media dan institusi. Dengan demikian, penyebaran konten deepfake telah memberikan dampak yang luas—baik secara sosial, politik, maupun ekonomi—dan mengancam kepercayaan publik dalam mengonsumsi informasi digital. Upaya mitigasi yang terpadu menjadi sangat penting agar teknologi ini dapat diarahkan pada penggunaan yang lebih etis dan produktif, serta tidak menjadi alat manipulatif yang merusak tatanan sosial.

6. Jenis Konten yang Sering di Manipulasi

Salah satu bentuk konten yang sering dimanipulasi dengan menggunakan teknologi kecerdasan buatan adalah deepfake. Kasus penipuan yang melibatkan video deepfake dengan wajah Presiden Prabowo Subianto menjadi sorotan utama dalam diskusi mengenai ancaman teknologi digital dalam kejahatan siber. Dalam kasus tersebut, pelaku menggunakan teknologi AI untuk menciptakan video yang menampilkan wajah dan suara yang sangat menyerupai Presiden Prabowo, seolah-olah beliau secara langsung menawarkan bantuan keuangan kepada masyarakat. Video ini disebarluaskan melalui platform media sosial dan berhasil menarik perhatian publik, terutama karena tampilannya yang tampak autentik.

Kecepatan penyebaran dan tingkat kemiripan visual dan audio dari video deepfake tersebut menunjukkan betapa efektifnya teknologi ini dalam menipu masyarakat. Modus operandi ini mengungkapkan tantangan besar dalam mendeteksi serta menangkali penyalahgunaan teknologi deepfake di era digital. Kasus ini menegaskan urgensi untuk merumuskan regulasi dan mekanisme verifikasi yang lebih ketat guna memastikan keaslian konten digital, khususnya yang melibatkan figur publik.

Selain Presiden Prabowo, pelaku juga memanfaatkan identitas Wakil Presiden Gibran Rakabuming Raka dan Menteri Keuangan Sri Mulyani dalam video serupa. Hal ini menunjukkan bahwa pelaku tidak ragu menggunakan citra pejabat tinggi negara untuk mencapai tujuan penipuan mereka. Dengan memanfaatkan kecanggihan teknologi, konten palsu dapat dibuat secara meyakinkan sehingga korban lebih mudah terperdaya. Oleh karena itu, kewaspadaan masyarakat terhadap informasi yang diterima, terutama dari sumber tidak resmi, menjadi sangat penting. Selain itu, kolaborasi antara pemerintah, penyedia platform media sosial, dan masyarakat diperlukan untuk meningkatkan literasi digital demi meminimalkan dampak negatif dari penyebaran informasi palsu berbasis deepfake (Yoan, Jasmin dkk 2025)



7. Peran Hukum di Indonesia Dalam Menangani Deepfake

Melihat tingginya potensi penyalahgunaan teknologi deepfake, terutama dalam bentuk deepfake porn, maka penting untuk meninjau sejauh mana kerangka hukum di Indonesia mampu merespons fenomena ini. Penyalahgunaan teknologi deepfake, khususnya dalam

bentuk deepfake porn, menimbulkan tantangan hukum dan etika yang kompleks. Kasus-kasus yang melibatkan manipulasi visual dan audio untuk tujuan pornografi, pencemaran nama baik, atau pemerasan telah mengaburkan batas antara kebebasan berekspresi dan pelanggaran privasi. Di Indonesia, bentuk kejahatan ini dapat dikaitkan dengan beberapa regulasi, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pornografi, Undang-Undang Perlindungan Data Pribadi (UU PDP), serta Kitab Undang-Undang Hukum Pidana (KUHP) yang baru.

Meski demikian, belum ada regulasi yang secara eksplisit mengatur deepfake sebagai objek hukum. UU ITE, misalnya, mengatur distribusi konten asusila dan informasi bohong, tetapi tidak secara spesifik menyebutkan konten hasil rekayasa AI. Begitu pula UU PDP yang fokus pada perlindungan data pribadi, belum menjawab secara langsung permasalahan rekayasa citra dan suara individu menggunakan AI. Oleh karena itu, diperlukan pembaruan dan harmonisasi hukum untuk menjangkau dimensi baru dari kejahatan digital. Selain pendekatan hukum, peningkatan kesadaran publik menjadi strategi penting dalam pencegahan penyalahgunaan deepfake. Literasi digital yang kuat dapat membantu masyarakat mengenali konten manipulatif dan menghindari penyebarannya. Edukasi ini tidak hanya penting bagi individu, tetapi juga bagi institusi seperti sekolah, organisasi, dan perusahaan yang mungkin menjadi target atau perantara penyebaran konten palsu. Upaya ini dapat dilakukan melalui pelatihan, kampanye digital, serta kolaborasi dengan platform media sosial (Andhika, Prama 2023).

Karena sifat kejahatan deepfake yang lintas negara, kerja sama internasional juga perlu diperkuat, baik melalui perjanjian bilateral maupun multilateral. Hal ini mencakup pertukaran data intelijen, penyelarasan hukum antarnegara, dan pengembangan standar etika teknologi global. Selain itu, mekanisme pelaporan dan perlindungan korban juga harus diperkuat. Korban perlu diberi akses terhadap dukungan hukum dan psikologis, serta hak untuk menuntut penghapusan konten yang melanggar privasinya. Dengan menggabungkan pendekatan yuridis, edukatif, dan kolaboratif, serta membangun regulasi yang adaptif terhadap perkembangan teknologi, Indonesia dapat memperkuat upaya pencegahan dan penanggulangan terhadap kejahatan deepfake. Hal ini penting untuk menjaga integritas digital, martabat individu, dan stabilitas sosial di era teknologi canggih.

KESIMPULAN

Teknologi deepfake merupakan inovasi berbasis kecerdasan buatan (AI) yang memungkinkan manipulasi konten audio, video, gambar, bahkan teks, sehingga tampak seolah-olah autentik padahal palsu. Meskipun awalnya dikembangkan untuk keperluan hiburan dan riset, dalam perkembangannya deepfake menimbulkan banyak kekhawatiran, khususnya dalam aspek sosial, keamanan, dan hukum. Dampak negatif dari deepfake sangat signifikan, mulai dari penyebaran informasi palsu, penipuan finansial, perusakan reputasi, hingga pelanggaran privasi seperti dalam kasus deepfake porn. Di Indonesia, fenomena ini semakin marak dengan mudahnya akses terhadap data digital serta kurangnya literasi digital masyarakat. Penggunaan deepfake untuk manipulasi politik, pencemaran nama baik, hingga penyebaran hoaks menjadi ancaman nyata yang dapat merusak tatanan sosial dan mengganggu kepercayaan publik terhadap informasi digital.

DAFTAR PUSTAKA

- A. (2024). Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban. *Media Hukum Indonesia (MHI)*, 2(2).
- A. AMALIA. NILA. and MHD. TAUFAN. H (2022) Deteksi Video Deepfake Menggunakan Convolutional Neural Network Model Resnet50 Undergraduate (S-1) thesis, Universitas Mikroskil.
- Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., & Li, H. (2020). Protecting World Leaders Against Deep Fakes. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*.
- Amelia, Y. F., Kaimuddin, A., & Ashsyarofi, H. L. (2024). Pertanggungjawaban pidana pelaku terhadap korban penyalahgunaan artificial intelligence deepfake menurut Hukum positif Indonesia. *Dinamika*, 30(1), 9675-9691.
- Andriani, R. (2022). *Ancaman Deepfake Audio dalam Kejahatan Siber di Indonesia*. Jakarta: Pusat Studi Siber dan Forensik Digital Indonesia.
- Ardiyani, N. K. D. I. (2024). Analisis Yuridis Pertanggungjawaban Pidana Pelaku Deepfake Porn Berdasarkan Hukum Positif. *Jurnal Kajian Hukum Dan Kebijakan Publik* | E-ISSN: 3031-8882, 2(1), 603-608.
- Chairani, M. A., Yitawati, K., & Pradhana, A. P. (2024). Urgensi pengaturan hukum bagi penyalahgunaan aplikasi deepfake. *Jurnal Rechtsens*, 13(1), 81-96.
- Chairani, M. A., Yitawati, K., & Pradhana, A. P. (2024). Urgensi pengaturan hukum bagi penyalahgunaan aplikasi deepfake. *Jurnal Rechtsens*, 13(1), 81-96.
- Darmawan, M. T., Junaidi, A., & Khaerudin, A. (2025). Penegakan Hukum Terhadap Penyalahgunaan Deepfake Pada Pornografi Anak Di Era Artificial Intelligence di Indonesia. *JURNAL PENELITIAN SERAMBI HUKUM*, 18(01), 42-54.
- Dewi, A. S., & Setiawan, D. A. (2024, January). Penegakan Hukum Terhadap Pelaku Tindak Pidana Video Deepfake Porn Dihubungkan Hukum Pidana Postif Di Indonesia. In *Bandung Conference Series: Law Studies (Vol. 4, No. 1, pp. 510-514)*.
- Fadillah, N. M. F., & Setiawan, H. DAMPAK TEKNOLOGI DEEPPFAKE TERHADAP KEPERCAYAAN PUBLIK DAN PENYEBARAN INFORMASI DI MEDIA SOSIAL.
- Haida, R. S. N., & Nuriyatman, E. (2024). URGENSI PENGATURAN PERLINDUNGAN HUKUM TERHADAP KORBAN DEEPPFAKE MELALUI ARTIFICIAL INTELIGENCE (AI) DARI PERSPEKTIF HUKUM PIDANA INDONESIA. *Jurnal Hukum Respublica*, 24(01).
- Hasan, K., Husna, A., Muchlis, M., Fitri, D., & Zulfadli, Z. (2023). Transformasi komunikasi massa era digital antara peluang dan tantangan. *JPP Jurnal Politik dan Pemerintahan*, 8(1), 41-55.
- Hendrawan, A. (2021). *Teknologi Deepfake dan Implikasinya terhadap Opini Publik di Indonesia*. Bandung: Penerbit Informatika.
- Mongkau, N. H., Bawole, H. Y. A., & Musa, A. (2025). PENEGAKKAN HUKUM TERHADAP PENYALHGUNAAN KECERDASAN BUATAN DENGAN CARA MEMANIPULASI WAJAH SESEORANG KE DALAM GAMBAR ATAU VIDEO PORNO. *LEX ADMINISTRATUM*, 13(2).
- Rendy Pasalbesy. (2019). *Perilaku Dasar Deepfake*. Fakultas Hukum Unpatti, Ambon

Respati, A. A., Setyarini, A. D., Parlagutan, D., Rafli, M., Mahendra, R. S., & Nugroho, A.

Sijabat, S. A. U., & Lukitasari, D. (2024). Konten gambar dan video pornografi deepfake sebagai suatu bentuk tindak pidana pencemaran nama baik. *Recidive*, 13(2), 179–180.

Utama N.A, Kesuma T.P dan Hidayat M.R, 2023. Analisis hukum terhadap upaya pencegahan kasus deepfake porn dan pendidikan kesadaran publik lingkungan.