JURNAL HUKUM DAN KONSTITUSI JIC

https://anwarpublisher.com/index.php/jic Volume 1 Nomor 3 Tahun 2025, hal.132-146

PENGGUNAAN *ARTIFICIAL INTELLIGENCE* DAN *DEEP FAKE* ANALISIS KASUS PIDANA VIDEO *DEEPFAKE* YANG MENCATUT PRESIDEN PRABOWO SUBIANTO TAHUN 2025

Muhammad Gilang Ramadhan Nur Hermansyah

[1] *Politeknik Pengayoman Indonesia*
Corresponding Author: Muhammad Gilang Ramadhan Nur Hermansyah, Email: myssess@gmail.com

Abstract

The rapid development of Artificial Intelligence (AI) has enabled the creation of sophisticated digital content, including deepfake technology that can manipulate a person's face and voice with high realism. Although it offers positive potential, this technology is also vulnerable to misuse for fraud and the dissemination of disinformation. The deepfake case involving the name of President Prabowo Subianto in 2025 illustrates how such technology can disrupt the integrity of public information and create social unrest. Based on this context, this study aims to analyze the use of AI in producing deepfake videos and examine their legal implications in Indonesia. This research employs a descriptive qualitative method with a case study approach. Data were collected through literature review of statutory regulations, official police reports, online news sources, and academic studies related to deepfake technology and the application of the Electronic Information and Transactions Law (UU ITE). Content analysis techniques were used to assess the legal facts and social impacts arising from the case. The findings indicate that the perpetrator's actions fulfill the elements of criminal offenses under Article 35 in conjunction with Article 51 paragraph (1) of the UU ITE, as well as Article 378 of the Indonesian Criminal Code concerning fraud. The study concludes that preventing the misuse of deepfake technology requires strengthened regulation, improved digital literacy, and enhanced cyber-forensic capabilities.
Keywords: *Deepfake, Artificial Intelligence, Cyber Law.*

Abstrak

Perkembangan teknologi *Artificial Intelligence* (AI) telah memberikan kemudahan dalam produksi konten digital, termasuk teknologi *deepfake* yang mampu memanipulasi wajah dan suara seseorang secara sangat realistis. Namun, kemajuan ini juga menimbulkan ancaman baru, terutama ketika digunakan untuk tujuan penipuan dan penyebaran disinformasi. Salah satu kasus yang menyoroti penyalahgunaan teknologi tersebut adalah *video deepfake* yang mencatut nama Presiden Prabowo Subianto pada tahun 2025. Kasus ini menimbulkan keresahan publik dan menunjukkan lemahnya literasi digital masyarakat dalam mengenali manipulasi visual berbasis AI. Tujuan penelitian ini untuk menganalisis penggunaan AI dalam pembuatan deepfake dan implikasi hukumnya di Indonesia. Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi kasus. Data diperoleh melalui studi literatur terhadap sumber hukum, laporan resmi kepolisian, pemberitaan daring, dan kajian akademik terkait teknologi deepfake dan regulasi UU ITE. Analisis dilakukan menggunakan teknik analisis isi untuk meninjau fakta hukum dan dampak sosial yang ditimbulkan. Hasil penelitian menunjukkan bahwa perbuatan pelaku memenuhi unsur tindak pidana dalam Pasal 35 Jo Pasal 51 ayat (1) UU ITE tentang manipulasi data elektronik serta Pasal 378 KUHP mengenai penipuan. Penyebaran deepfake juga berpotensi menciptakan ketidakstabilan informasi dan menurunkan tingkat kepercayaan masyarakat terhadap media digital. Kesimpulannya, penguatan regulasi, peningkatan literasi digital, serta pengembangan kemampuan forensik siber menjadi langkah penting untuk mencegah penyalahgunaan teknologi deepfake di masa depan.
Kata Kunci: Deepfake, Artificial Intelligence, Hukum Siber.

Volume 1 Nomor 3 Tahun 2025

Article Information : *Received: 02 Maret 2025* *Accepted: 1 Juni 2025*

1. Pendahuluan

Perkembangan teknologi digital pada abad ke-21 telah membawa perubahan besar dalam berbagai aspek kehidupan manusia, terutama dalam bidang komunikasi, informasi, dan sistem hukum. Revolusi digital yang ditandai dengan kehadian Artificial Intelligence (AI) atau kecerdasan buatan telah memungkinkan mesin untuk meniru kemampuan kognitif manusia, seperti belajar, menganalisis pola, dan mengambil keputusan secara mandiri. Menurut laporan McKinsey Global Institute, perkembangan AI diprediksi mampu meningkatkan produktivitas global hingga 1,2% per tahun karena kemampuannya mengotomatisasi pekerjaan yang sebelumnya hanya dapat dilakukan manusia (MGI, 2023). Di Indonesia, pemanfaatan AI juga meningkat pesat dalam sektor pemerintahan, pendidikan, finansial, hingga pelayanan publik. Namun, kemajuan ini tidak hanya membawa manfaat positif, tetapi juga membuka ruang baru bagi risiko, salah satunya penyalahgunaan teknologi berbasis AI bernama deepfake[1].

Deepfake merupakan hasil manipulasi gambar, suara, atau video yang dibuat menggunakan algoritma deep learning, khususnya Generative Adversarial Networks (GAN). Menurut Goodfellow (2014), GAN bekerja melalui kompetisi dua jaringan saraf (generator dan discriminator) sehingga mampu menghasilkan konten palsu yang sangat realistis. Teknologi deepfake kini menjadi fenomena global yang mengancam kepercayaan publik, karena konten palsu yang dihasilkan sering digunakan untuk menyebarkan misinformasi, propaganda politik, hingga penipuan digital (digital fraud). Laporan Europol (2022) bahkan menyebutkan bahwa 90% konten digital dapat dimanipulasi pada tahun 2026 jika tidak diimbangi dengan sistem deteksi yang kuat.

Indonesia turut merasakan dampak dari maraknya teknologi deepfake. Fenomena ini mencapai puncaknya pada tahun 2025 ketika beredar video deepfake yang mencatut nama Presiden Prabowo Subianto dan Menteri Keuangan Sri Mulyani. Dalam video tersebut, Presiden tampak mengumumkan sebuah program bantuan pemerintah padahal seluruh visual dan audio merupakan manipulasi AI. Masyarakat diarahkan untuk melakukan transfer sejumlah uang sebagai biaya administrasi ke rekening yang telah disiapkan pelaku. Menurut laporan Direktorat Tindak Pidana Siber Bareskrim Polri, ribuan warga menjadi korban karena video tersebut disebarkan secara masif melalui platform media sosial dan aplikasi pesan instan (AFP, 2025). Setelah penyelidikan, pelaku berinisial AMA dan JS berhasil ditangkap, dan kasus ini menjadi contoh nyata bagaimana teknologi deepfake dapat dimanfaatkan sebagai sarana penipuan yang meresahkan masyarakat[2].

Kasus tersebut menunjukkan bahwa persoalan deepfake bukan hanya masalah teknis terkait kecanggihan algoritma AI, tetapi juga masalah sosial, hukum, serta etika komunikasi publik. Dari sudut pandang teori komunikasi, fenomena ini dapat dijelaskan menggunakan Media Manipulation Theory, yang menyatakan bahwa perkembangan media digital memungkinkan munculnya manipulasi konten secara sistematis untuk memengaruhi persepsi publik (Nissen, 2020). Selain itu, Disinformation Theory relevan untuk menjelaskan bagaimana konten palsu diproduksi dan didistribusikan untuk menghasilkan kerugian, kekacauan, atau keuntungan tertentu bagi pelaku. Secara kriminologis, kasus deepfake dapat dianalisis menggunakan Routine Activity Theory, yaitu bahwa kejahatan digital terjadi ketika ada pelaku yang termotivasi, target yang rentan, dan lemahnya pengawasan atau regulasi.

Dari perspektif penulis, kasus ini sekaligus menunjukkan bahwa masyarakat Indonesia masih memiliki tingkat literasi

[1] "Banyak Warga Jadi Korban Penipuan 'Deepfake' yang Catut Nama Prabowo – Suara Kalbar.CO.ID," 2025, https://www.suarakalbar.co.id/2025/03/banyak-warga-jadi-korban-penipuan-deepfake-yang-catut-nama-prabowo/.

[2] "Bareskrim Tangkap Pelaku Penipuan Deepfake AI, Catut Nama Pejabat Negara," 2025, https://www.metrotvnews.com/read/K5nC7p3d-bareskrim-tangkap-pelaku-penipuan-deepfake-ai-catut-nama-pejabat-negara.

digital yang relatif rendah, terutama dalam mengenali konten manipulatif berbasis AI. Banyak warga masih menganggap bahwa video adalah bukti paling valid dari suatu informasi, sehingga tidak mencurigai keaslian visual yang beredar. Di sisi lain, perangkat hukum nasional seperti UU ITE dan KUHP masih perlu diperkuat agar mampu mengakomodasi bentuk-bentuk kejahatan digital baru yang memanfaatkan teknologi generatif[3].

Oleh karena itu, penelitian atau kajian mengenai kasus video deepfake yang mencatut nama Presiden Prabowo Subianto pada tahun 2025 menjadi sangat penting. Pembahasan ini tidak hanya relevan untuk memahami bagaimana hukum Indonesia merespons fenomena deepfake, tetapi juga untuk melihat bagaimana teknologi, masyarakat, dan sistem hukum saling berinteraksi dalam konteks era digital. Makalah ini akan menganalisis aspek teknologi deepfake, implikasi hukumnya, dampak sosialnya terhadap masyarakat, serta upaya penanggulangan yang dapat dilakukan oleh negara dan institusi terkait. Dengan demikian, kajian ini diharapkan mampu memberikan gambaran komprehensif mengenai tantangan hukum dan komunikasi publik di era kecerdasan buatan yang semakin maju.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi kasus terhadap peristiwa penyebaran video *deepfake* yang mencatut nama Presiden Prabowo Subianto tahun 2025. Data dikumpulkan melalui studi literatur, yaitu penelusuran berita resmi, laporan kepolisian, peraturan perundang-undangan (UU ITE dan KUHP), serta sumber ilmiah terkait teknologi Artificial Intelligence dan deepfake. Analisis dilakukan dengan teknik analisis isi (content analysis) untuk menafsirkan makna, dampak sosial, serta implikasi hukum dari kasus tersebut, sehingga diperoleh pemahaman yang komprehensif dan kontekstual.

3. Hasil dan Pembahasan

a. Pengertian dan Karakteristik *Artificial Intelligence* dan *Deepfake*

Perkembangan teknologi informasi dan komunikasi telah membawa manusia pada era baru di mana batas antara realitas dan rekayasa digital menjadi semakin kabur. Salah satu hasil kemajuan tersebut adalah Artificial Intelligence (AI) atau kecerdasan buatan, yang memiliki kemampuan untuk meniru perilaku kognitif manusia. AI kini tidak hanya digunakan dalam bidang industri, ekonomi, maupun pendidikan, tetapi juga telah merambah ke dunia hiburan, media sosial, dan bahkan kejahatan siber. Salah satu manifestasi dari teknologi AI yang paling menimbulkan kontroversi adalah deepfake, yaitu teknologi manipulasi visual dan audio yang mampu membuat seseorang tampak mengatakan atau melakukan sesuatu yang sebenarnya tidak pernah dilakukan[4].

Secara umum, Artificial Intelligence adalah cabang ilmu komputer yang bertujuan untuk menciptakan mesin atau sistem yang mampu berpikir, belajar, dan mengambil keputusan layaknya manusia. AI bekerja dengan meniru cara kerja otak manusia melalui serangkaian algoritma matematis yang kompleks. Sistem AI belajar dari data yang diberikan, mengenali pola, kemudian menghasilkan keputusan atau keluaran yang relevan. Dalam perkembangannya, AI terbagi menjadi dua kategori besar: narrow AI (kecerdasan buatan terbatas), yang hanya mampu melakukan tugas spesifik seperti pengenalan wajah, terjemahan bahasa, atau rekomendasi konten; dan general AI (kecerdasan buatan umum), yaitu sistem yang mampu berpikir dan memahami konteks secara luas seperti manusia. Saat ini, teknologi

[3] Nadiyah Nadiyah, Ronny Winarno, dan Wiwin Ariesta, "Kajian Hukum Terhadap Penggunaan Artificial Intelligence (AI) Yang Berakibat Menyerang Kehormatan," *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory* 3, no. 3 (Juli 2025): 2415–22, https://doi.org/10.62976/ijijel.v3i3.1287.

[4] Kadek Melda Luxiana, "Bareskrim Limpahkan Berkas 2 Tersangka Deepfake Catut Prabowo ke Kejaksaan," Detiknews, 2025, https://news.detik.com/berita/d-7883615/bareskrim-limpahkan-berkas-2-tersangka-deepfake-catut-prabowo-ke-kejaksaan.

deepfake termasuk dalam kategori narrow AI karena dirancang khusus untuk memanipulasi dan merekayasa citra visual serta audio.

Istilah deepfake berasal dari gabungan kata deep learning dan fake. Deep learning sendiri merupakan cabang dari machine learning (pembelajaran mesin) yang menggunakan jaringan saraf tiruan atau artificial neural networks untuk menganalisis data dalam jumlah besar. Dalam konteks deepfake, teknologi ini bekerja dengan menggunakan algoritma Generative Adversarial Network (GAN), yaitu sistem yang melibatkan dua jaringan AI yang saling berkompetisi. Jaringan pertama, disebut generator, bertugas menciptakan gambar atau video palsu yang menyerupai aslinya. Sedangkan jaringan kedua, disebut discriminator, berfungsi mendeteksi keaslian dari hasil tersebut. Proses ini dilakukan berulang kali hingga video palsu yang dihasilkan tampak sangat realistis dan sulit dibedakan dari video asli[5].

Secara karakteristik, deepfake memiliki beberapa ciri utama. Pertama, hasil manipulasi visual dan audio yang dihasilkan tampak autentik dan sulit dideteksi secara kasatmata. Gerakan bibir, ekspresi wajah, hingga intonasi suara dapat disesuaikan sedemikian rupa sehingga seolah-olah seseorang benar-benar mengucapkan kata atau melakukan tindakan tertentu. Kedua, pembuatan deepfake semakin mudah dilakukan karena banyaknya perangkat lunak open-source dan aplikasi berbasis AI yang tersedia secara publik. Hal ini menyebabkan siapa pun dengan keterampilan komputer dasar dapat memproduksi konten deepfake hanya dengan menggunakan ponsel atau laptop pribadi. Ketiga, konten deepfake mudah menyebar di media sosial karena sifatnya yang menarik dan sensasional, sehingga memiliki potensi besar untuk menimbulkan disinformasi dan kerugian sosial. Meskipun deepfake memiliki potensi positif, seperti dalam bidang perfilman, pelatihan medis, atau pelestarian sejarah digital, penggunaan teknologi ini tanpa etika dapat berbahaya. Deepfake dapat digunakan untuk menyebarkan hoaks, melakukan penipuan daring, pemerasan, atau merusak reputasi seseorang. Dalam konteks hukum dan sosial, deepfake mengaburkan batas antara kebenaran dan kebohongan, serta mengancam kredibilitas tokoh publik maupun institusi pemerintah. Oleh karena itu, diperlukan pemahaman mendalam dan kebijakan yang bijak dalam memanfaatkan kecerdasan buatan agar inovasi ini tidak berubah menjadi ancaman bagi keamanan informasi dan kepercayaan publik.

Dengan demikian, Artificial Intelligence dan deepfake merupakan dua fenomena teknologi yang saling terkait erat. AI menjadi fondasi yang memungkinkan terciptanya deepfake, sedangkan deepfake menjadi contoh nyata dari bagaimana kemampuan AI dapat disalahgunakan. Kecanggihan ini menuntut kesiapan hukum, moral, dan sosial masyarakat dalam menghadapi era digital yang semakin kompleks[6].

Untuk kajian akademik, beberapa teori berikut sering digunakan dalam menganalisis AI dan deepfake[7]:

1. Teori *Machine Learning* dan *Deep Learning*
   1) Menjelaskan bagaimana algoritma belajar dari data.
   2) Terutama Deep Neural Networks (DNN) dan Convolutional Neural Networks (CNN).
2. Teori Generative Adversarial Networks (GAN) (Goodfellow, 2014)
   1) Teori paling relevan dalam penjelasan deepfake.

[5] Adnasohn Aqilla Respati, "Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation," *Jurnal USM Law Review* 7, no. 3 (Desember 2024): 1737–58, https://doi.org/10.26623/julr.v7i3.10578.

[6] Maria Karunia Putri Maan, Heryanto Amalo, dan Ngongo Dede, "Analisis Perlindungan Hukum terhadap Penyimpangan Artificial Intelligence dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana," *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora* 4, no. 1 (Januari 2025): 296–307, https://doi.org/10.55606/jurrish.v4i1.5071.

[7] Muhammad Nur Hidayat, "Pertanggungjawaban Pidana Terhadap Penyalahgunaan Deepfake Sebagai Ancaman Keamanan Data Pribadi," *UNES Law Review* 7, no. 4 (Juli 2025): 2036–48, https://doi.org/10.31933/unesrev.v7i4.2433.

2) GAN terdiri dari dua jaringan:
   a) Generator → membuat gambar/video manusia palsu.
   b) Discriminator → menilai apakah gambar/video itu asli atau palsu.
3) GAN terus berkompetisi sehingga menghasilkan manipulasi yang sangat realistis.

3. Teori Media Manipulation (Media Theory)

Berkaitan dengan bagaimana teknologi memengaruhi informasi digital. Deepfake dipandang sebagai bentuk manipulasi media berbasis teknologi yang dapat memengaruhi persepsi publik.

4. Teori Disinformasi dan Misinformasi

Digunakan untuk menjelaskan bagaimana deepfake digunakan untuk membentuk opini publik atau menipu masyarakat.

5. Teori Kejahatan Dunia Maya (Cybercrime Theory)

Terkait penggunaan deepfake untuk tujuan ilegal, misalnya:

1) Routine Activity Theory
2) Opportunity Theory
3) Deterrence Theory dalam pencegahan kejahatan digital.

6. Teori Etika Teknologi (Techno-Ethics)

Membahas dampak etis AI dan deepfake terhadap privasi, identitas, dan integritas informasi.

b. Kronologi Kasus Deepfake yang Mencatut Presiden Prabowo Subianto

Kasus penyalahgunaan teknologi deepfake yang mencatut nama Presiden Prabowo Subianto menjadi salah satu peristiwa menonjol di Indonesia pada tahun 2025. Kasus ini menunjukkan bagaimana kemajuan teknologi kecerdasan buatan (Artificial Intelligence/AI) dapat dimanfaatkan untuk tindak kejahatan siber berupa penipuan dan penyebaran disinformasi. Peristiwa ini tidak hanya menimbulkan kerugian ekonomi bagi masyarakat, tetapi juga mengancam kepercayaan publik terhadap pejabat negara dan lembaga pemerintahan. Awal mula kasus ini terungkap pada Januari 2025, ketika Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri menerima laporan dari sejumlah masyarakat yang merasa tertipu oleh video yang menampilkan sosok Presiden Prabowo Subianto. Dalam video tersebut, tampak Presiden Prabowo berbicara kepada masyarakat mengenai program bantuan pemerintah dan mengajak warga untuk mendaftar melalui tautan atau nomor WhatsApp yang disertakan dalam unggahan. Video itu tersebar luas di platform Instagram dan TikTok, dengan berbagai judul seperti "Prabowo Berbagi" atau "Prabowo Giveaway". Bagi orang awam, video tersebut terlihat sangat meyakinkan; mulut Prabowo tampak bergerak selaras dengan suara yang terdengar, ekspresi wajahnya pun realistis, sehingga banyak warga tidak menyadari bahwa konten tersebut hasil manipulasi digital.

Setelah dilakukan penyelidikan, polisi berhasil menangkap pelaku pertama berinisial AMA (29 tahun) pada 16 Januari 2025 di wilayah Lampung Tengah. Beberapa minggu kemudian, hasil pengembangan kasus mengarah pada tersangka kedua berinisial JS (25 tahun), yang ditangkap di Kabupaten Pringsewu, Provinsi Lampung, pada 4 Februari 2025. Keduanya terbukti sebagai pihak yang menyebarluaskan video deepfake yang mencatut nama Presiden Prabowo dan Menteri Keuangan Sri Mulyani Indrawati[8].

Menurut keterangan Brigjen Pol. Himawan Bayu Aji, selaku Direktur Tindak Pidana Siber Bareskrim Polri, tersangka JS mengelola akun Instagram @indoberbagi2025 dengan lebih dari 9.399 pengikut. Dalam akun tersebut, JS mengunggah video deepfake yang menampilkan Presiden Prabowo seolah-olah sedang mengumumkan program bantuan sosial untuk masyarakat. Dalam keterangan video, pelaku menuliskan imbauan agar warga yang ingin menerima bantuan segera mendaftar melalui nomor WhatsApp yang ia cantumkan. Setelah korban menghubungi nomor tersebut, pelaku akan meminta mereka mengisi data pribadi dan kemudian diminta mentransfer sejumlah uang antara Rp250.000

[8] Sabrina Nur Syahirah dan Bayu Prasetyo, "Tinjauan Yuridis Terhadap Penggunaan Teknologi Deepfake Untuk Pornografi Melalui Artificial Intelligence (AI) Di Indonesia," *Jurnal Inovasi Hukum Dan Kebijakan* 6, no. 1 (2025).

hingga Rp1.000.000 dengan alasan "biaya administrasi pencairan bantuan". Namun, bantuan yang dijanjikan tidak pernah ada, dan uang tersebut langsung masuk ke rekening pelaku[9].

Hasil penyelidikan menunjukkan bahwa video deepfake tersebut tidak dibuat sendiri oleh pelaku, melainkan diunduh dari akun media sosial lain menggunakan kata kunci "Prabowo Giveaway". Setelah itu, JS mengunggah ulang video tersebut dengan tambahan keterangan dan nomor kontak pribadi untuk menjaring korban. Dengan cara ini, ia berhasil menipu lebih dari 100 orang korban dari 20 provinsi di Indonesia. Korban terbanyak berasal dari Jawa Timur, Jawa Tengah, dan Papua, dengan total keuntungan yang diperoleh pelaku mencapai sekitar Rp65 juta.

Dari hasil analisis digital forensik, tim penyidik menemukan bahwa video yang digunakan merupakan hasil manipulasi berbasis Generative Adversarial Network (GAN), teknologi utama di balik deepfake. Analisis dilakukan menggunakan dua perangkat lunak forensik video yang berbeda dan menunjukkan nilai 100% fake, dengan skor deteksi 1.00 dalam pengujian deepfake face detection, yang merupakan indikator tertinggi dari hasil rekayasa visual. Artinya, video tersebut sepenuhnya hasil sintesis AI dan bukan rekaman asli.

Selain akun Instagram @indoberbagi2025, ditemukan pula beberapa akun pendukung di platform TikTok dan Facebook yang memposting video serupa. Bahkan, tim Fact-Check AFP menemukan bahwa fenomena penyebaran video deepfake Prabowo telah meluas sejak akhir 2024, dengan puluhan akun memposting konten manipulatif serupa. Beberapa di antaranya bahkan memanfaatkan momen pelantikan Prabowo sebagai Presiden untuk menarik simpati publik dan menjaring korban dengan modus yang sama. Salah satu akun dengan lebih dari 77.000 pengikut berhasil memperoleh 7,5 juta tayangan melalui video deepfake yang menawarkan bantuan palsu atas nama Presiden.

Setelah dilakukan penyidikan lebih lanjut, Bareskrim Polri melimpahkan berkas perkara tahap II kepada kejaksaan pada 24 April 2025. Pelaku AMA diserahkan ke Kejaksaan Negeri Lampung Tengah, sedangkan JS dilimpahkan ke Kejaksaan Agung karena dinilai memiliki jaringan lebih luas. Keduanya dijerat dengan Pasal 51 ayat (1) jo Pasal 35 UU ITE dan Pasal 378 KUHP tentang Penipuan, dengan ancaman pidana hingga 12 tahun penjara dan/atau denda maksimal Rp12 miliar.

Selain kedua pelaku tersebut, penyelidikan lanjutan juga menemukan kasus serupa yang melibatkan nama pejabat lain, seperti Gubernur Jawa Timur Khofifah Indar Parawansa, yang dimanipulasi dalam video deepfake di TikTok untuk menipu masyarakat dengan modus penjualan sepeda motor murah. Kasus ini diungkap oleh Ditreskrimsus Polda Jawa Timur pada 16 April 2025, yang menangkap tiga pelaku asal Pangandaran, Jawa Barat. Polri menegaskan bahwa penyalahgunaan teknologi AI untuk kejahatan digital kini menjadi pola baru yang membutuhkan pengawasan lebih intensif.

Menanggapi fenomena ini, Polri bekerja sama dengan Kementerian Komunikasi dan Digital (Kemenkom Digi) untuk melakukan pemblokiran dan penurunan (takedown) terhadap akun-akun penyebar video deepfake. Selain itu, patroli siber terus ditingkatkan untuk mencegah penyebaran hoaks berbasis AI di media sosial. Brigjen Himawan juga mengimbau masyarakat agar lebih waspada terhadap video atau pesan yang mencatut nama pejabat negara, terutama jika mengandung unsur permintaan uang atau data pribadi.

Kasus ini menjadi pelajaran penting bagi Indonesia bahwa kemajuan teknologi AI tidak hanya membawa manfaat, tetapi juga menghadirkan tantangan baru dalam bidang hukum dan keamanan digital. Penyalahgunaan

[9] Almira Daisy Zahrah Fadhilah dan Sri Retnoningsih, "Perancangan Kampanye Digital Melawan Disinformasi Melalui Artificial Intelligence Dan Deepfake Di Kalangan Pra Lansia Usia 45-55 Tahun," *FAD* 3, no. 02 (Juli 2024), https://eproceeding.itenas.ac.id/index.php/fad/article/view/2943.

deepfake sebagai alat penipuan membuktikan perlunya edukasi publik, peningkatan literasi digital, serta penguatan kemampuan forensik siber dalam menghadapi ancaman manipulasi berbasis kecerdasan buatan[10].

c. Modus Operandi dan Analisis Teknologi yang Digunakan

Kasus penyebaran video deepfake yang mencatut nama Presiden Prabowo Subianto pada tahun 2025 memperlihatkan bagaimana teknologi kecerdasan buatan dapat dimanfaatkan untuk tujuan kriminal. Dalam konteks ini, pelaku menggunakan Artificial Intelligence (AI) untuk memanipulasi wajah dan suara tokoh publik, kemudian menyebarkannya melalui media sosial guna menipu masyarakat. Pemahaman terhadap modus operandi dan teknologi yang digunakan menjadi penting agar upaya pencegahan dan penegakan hukum dapat dilakukan secara lebih efektif[11].

1. Pola Umum dan Tahapan Modus Operandi

Pelaku dalam kasus ini, yaitu JS dan AMA, menjalankan penipuan dengan metode yang terstruktur. Berdasarkan hasil penyelidikan Dittipidsiber Bareskrim Polri, terdapat beberapa tahapan utama dalam modus operandi yang mereka lakukan:

1) Pengumpulan dan Pemilihan Video Asli

Pelaku terlebih dahulu mencari dan mengunduh video resmi Presiden Prabowo dari sumber publik, seperti pidato kenegaraan, wawancara, atau rekaman acara resmi. Video asli ini berfungsi sebagai bahan dasar untuk manipulasi. Pelaku kemudian memilih cuplikan dengan kualitas visual yang baik agar proses rekayasa wajah lebih halus dan realistis.

2) Pemanfaatan Teknologi Deepfake

Setelah mendapatkan video dasar, pelaku menggunakan perangkat lunak berbasis Generative Adversarial Network (GAN) untuk mengganti wajah dan suara asli dengan versi manipulatif. Dalam kasus ini, wajah dan suara Presiden dimodifikasi agar seolah-olah sedang memberikan pernyataan tertentu, seperti ajakan mengikuti program bantuan sosial atau hadiah pemerintah.

3) Pembuatan Narasi Penipuan

Setelah video deepfake selesai, pelaku menambahkan teks atau narasi pendukung dalam deskripsi unggahan. Misalnya, ajakan untuk "mendaftar bantuan" atau "mengikuti giveaway dari Presiden". Pelaku juga menyertakan nomor WhatsApp pribadi atau tautan pendaftaran palsu agar korban mudah dihubungi dan diarahkan untuk melakukan transaksi.

4) Distribusi dan Promosi di Media Sosial

Video deepfake kemudian diunggah akun media sosial seperti Instagram (@indoberbagi2025) dan TikTok, dengan penggunaan tagar populer seperti #PrabowoBerbagi atau #BantuanPresiden. Pelaku memanfaatkan algoritma media sosial untuk menjangkau audiens yang lebih luas, terutama masyarakat berusia lanjut atau dengan literasi digital rendah.

5) Interaksi Langsung dengan Korban

Setelah korban tertarik, pelaku berkomunikasi melalui pesan pribadi dan meminta korban mengirimkan sejumlah uang sebagai "biaya administrasi" atau "pajak bantuan". Jumlah uang yang diminta bervariasi antara Rp250.000 hingga Rp1.000.000. Setelah korban mentransfer dana, pelaku menghapus atau memblokir kontak agar jejak digitalnya sulit dilacak. Modus seperti ini tergolong social engineering, yaitu strategi manipulasi psikologis untuk mengelabui korban agar melakukan tindakan tertentu. Pelaku memanfaatkan kepercayaan masyarakat terhadap figur publik dan ketidaktahuan terhadap teknologi deepfake[12].

2. Analisis Teknologi Deepfake yang Digunakan

[10] Muh Taufik Darmawan, Amir Junaidi, dan Ariy Khaerudin, "Penegakan Hukum Terhadap Penyalahgunaan Deepfake Pada Pornografi Anak Di Era Artifical Intelegence di Indonesia," *Jurnal Penelitian Serambi Hukum* 18, no. 01 (Januari 2025): 42–54, https://doi.org/10.59582/sh.v18i01.1257.

[11] AUNF Rahman, Syariffudin Syariffudin, dan Fathol Bari, "Perlindungan Hukum terhadap Korban Penyalahgunaan Teknik Deepfake," *Jurnal Perspektif Administrasi Publik dan Hukum* 2 (2025): 247–55.

[12] Maria Karunia Putri Maan, Heryanto Amalo, dan Ngongo Dede, "Analisis Perlindungan Hukum terhadap Penyimpangan Artificial Intelligence dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana."

Teknologi yang digunakan dalam kasus ini berbasis Artificial Intelligence (AI), khususnya cabang Deep Learning. Teknik utama yang digunakan adalah Generative Adversarial Network (GAN), yang merupakan model dua jaringan neural yang saling berkompetisi.

1) Generator bertugas membuat gambar atau video palsu berdasarkan data wajah dan suara target (dalam hal ini, Presiden Prabowo).
2) Discriminator bertugas menilai keaslian hasil yang dibuat oleh generator. Kedua jaringan ini berulang kali saling "menipu" hingga menghasilkan video yang tampak autentik dan sulit dibedakan dari video asli.

Dalam kasus JS, hasil analisis forensik video digital oleh Polri menunjukkan skor 1.00 dalam deteksi deepfake face detection, yang berarti 100% palsu. Manipulasi tersebut meliputi penggantian wajah, penyesuaian gerakan bibir, dan sinkronisasi suara. Hasil akhirnya menunjukkan wajah Presiden bergerak, berbicara, dan berekspresi seolah benar-benar mengucapkan kata-kata yang digunakan dalam narasi penipuan.

Selain itu, pelaku memanfaatkan perangkat lunak open-source deepfake yang dapat diunduh gratis dari internet. Software seperti DeepFaceLab atau FaceSwap memungkinkan pengguna dengan kemampuan dasar komputer untuk membuat video palsu hanya dalam waktu beberapa jam. Hal ini memperlihatkan bahwa pembuatan deepfake kini tidak lagi membutuhkan keahlian tinggi atau biaya besar.

3. Karakteristik Teknis dari Video Deepfake

Video deepfake yang digunakan pelaku memiliki beberapa karakteristik teknis yang khas:

1) Kualitas Visual Tinggi

Pelaku menggunakan resolusi video yang jernih untuk menyamarkan tanda-tanda manipulasi.

2) Sinkronisasi Bibir Akurat

Dengan bantuan model lip-sync, gerakan mulut disesuaikan secara tepat dengan audio yang dimasukkan.

3) Efek Cahaya dan Bayangan Realistis

Teknologi GAN menyesuaikan pencahayaan wajah agar serupa dengan latar video asli.

4) Durasi Pendek

Video biasanya berdurasi 30–60 detik agar penonton tidak sempat memperhatikan detail yang janggal.

5) Distribusi Cepat

Video disebarkan secara masif di berbagai platform untuk memperkuat persepsi bahwa konten tersebut otentik[13].

4. Dampak Teknologi terhadap Efektivitas Kejahatan

Keberhasilan modus ini tidak hanya bergantung pada kecanggihan teknologi, tetapi juga pada psikologi sosial dan kekurangan literasi digital masyarakat. Banyak korban tidak memahami bahwa AI dapat memalsukan wajah dan suara dengan sempurna. Kombinasi antara kredibilitas tokoh publik dan tampilan video realistis menciptakan efek trust illusion, yaitu keyakinan palsu terhadap kebenaran informasi. Selain itu, algoritma media sosial berperan mempercepat penyebaran konten semacam ini karena sistem rekomendasi otomatis menyoroti video yang memiliki interaksi tinggi, tanpa memperhatikan keaslian kontennya. Akibatnya, konten deepfake dengan unsur sensasional lebih mudah viral dibandingkan klarifikasi resmi dari pihak berwenang[14].

Modus operandi dalam kasus deepfake Prabowo menunjukkan bahwa teknologi AI dapat digunakan secara destruktif untuk kepentingan penipuan. Prosesnya melibatkan kombinasi antara rekayasa teknologi, manipulasi psikologis, dan eksploitasi kepercayaan sosial. Sementara itu, keberadaan perangkat lunak GAN menjadikan pembuatan video palsu semakin mudah, cepat, dan murah. Oleh karena itu, upaya pemberantasan kasus serupa harus melibatkan tiga pendekatan

[13] Respati, "Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation."

[14] Gelar Wirakusunah, "Pengembangan Media Pembelajaran Pengenalan Sejarah Pahlawan Indonesia Menggunakan Deep Fake Dengan Metode Multimedia Development Life Cycle," *Jurnal Informatika Dan Teknik Elektro Terapan* 12, no. 2 (April 2024), https://doi.org/10.23960/jitet.v12i2.4171.

sekaligus: penegakan hukum siber yang kuat, peningkatan literasi digital masyarakat, dan pengembangan sistem deteksi otomatis berbasis AI forensik. Kasus ini membuktikan bahwa dalam era digital, kejahatan tidak lagi hanya bergantung pada kekuatan fisik, tetapi juga pada kemampuan memanipulasi realitas menggunakan kecerdasan buatan[15].

d. Analisis Hukum terhadap Tindak Pidana Deepfake

Kasus penyebaran video deepfake yang mencatut nama Presiden Prabowo Subianto pada tahun 2025 menjadi bukti nyata bahwa kemajuan teknologi kecerdasan buatan (Artificial Intelligence/AI) tidak hanya membawa manfaat, tetapi juga menghadirkan tantangan hukum baru. Teknologi deepfake memungkinkan seseorang memanipulasi wajah dan suara tokoh publik secara realistis untuk tujuan tertentu, termasuk tindak penipuan. Oleh karena itu, analisis hukum terhadap perbuatan ini penting untuk memahami bagaimana regulasi di Indonesia mengatur dan menjerat pelaku penyalahgunaan teknologi AI dalam konteks kejahatan siber[16].

1. Landasan dan Penerapan Hukum terhadap Kasus Deepfake

Walaupun Indonesia belum memiliki undang-undang khusus yang secara eksplisit mengatur mengenai deepfake atau kecerdasan buatan, namun tindakan pelaku dalam kasus ini dapat dijerat melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah dengan UU Nomor 19 Tahun 2016, serta Kitab Undang-Undang Hukum Pidana (KUHP).

Dalam kasus ini, Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri menjerat dua pelaku, JS dan AMA, dengan Pasal 51 ayat (1) Jo Pasal 35 UU ITE dan Pasal 378 KUHP.

1) Pasal 35 UU ITE menyebutkan bahwa setiap orang yang dengan sengaja dan tanpa hak memanipulasi informasi elektronik dengan tujuan agar dianggap data yang otentik dapat dipidana.

   Dalam kasus deepfake, tindakan membuat video palsu dengan wajah dan suara Presiden Prabowo agar tampak seperti video asli memenuhi unsur "manipulasi informasi elektronik". Pelaku secara sadar menggunakan teknologi untuk menciptakan konten digital yang menyesatkan publik.

2) Pasal 378 KUHP tentang penipuan digunakan karena pelaku menggunakan martabat palsu dan tipu muslihat dengan tujuan memperoleh keuntungan pribadi. Video deepfake digunakan untuk meyakinkan korban agar mentransfer sejumlah uang dengan dalih biaya administrasi bantuan sosial. Kedua pasal tersebut diterapkan secara bersamaan karena perbuatan pelaku mengandung dua unsur tindak pidana sekaligus, yaitu pemalsuan digital dan penipuan konvensional. Berdasarkan pasal-pasal tersebut, pelaku diancam dengan pidana penjara maksimal 12 tahun dan/atau denda hingga Rp12 miliar.

2. Unsur-Unsur Pidana yang Terpenuhi

Berdasarkan analisis hukum, terdapat beberapa unsur penting yang terpenuhi dalam kasus deepfake Prabowo:

1) Unsur Kesengajaan (Mens Rea)

Pelaku JS dan AMA secara sadar membuat dan menyebarkan video palsu untuk menipu masyarakat. Mereka tidak hanya mengunggah video, tetapi juga menambahkan narasi yang mengarahkan korban untuk melakukan transfer uang.

2) Unsur Perbuatan Melawan Hukum (Actus Reus)

Manipulasi wajah dan suara tokoh publik dilakukan tanpa izin dan untuk tujuan

[15] Jesselyn Mu, Muhammad Adrezo, dan Ahmed Nizhan Haikal, "Identifikasi Wajah Asli Dan Buatan Deepfake Menggunakan Metode Convolutional Neural Network," *Teknika* 13, no. 1 (Januari 2024): 45–50, https://doi.org/10.34148/teknika.v13i1.705.

[16] Rambu Maharani dan Sri Maharani M.t.v.m, "Ganti Rugi Akibat Penyalahgunaan Artificial Intelligence (Deepfake) pada Citra Orang Terkenal di Facebook Berdasarkan Pasal 1365 BW," *Jurnal Hukum Lex Generalis* 6, no. 4 (April 2025), https://doi.org/10.56370/jhlg.v6i4.1512.

penipuan. Tindakan ini jelas melanggar hak privasi serta integritas citra pejabat negara.

3) Unsur Akibat

Tindakan pelaku menyebabkan kerugian nyata bagi masyarakat, baik secara materiil maupun immateriil. Lebih dari 100 orang menjadi korban penipuan dengan total kerugian sekitar Rp65 juta, selain menurunnya kepercayaan publik terhadap pemerintah.

Dengan terpenuhinya ketiga unsur tersebut, pelaku dapat dimintai pertanggungjawaban pidana penuh sesuai hukum yang berlaku.

3. Tantangan Penegakan Hukum di Era Teknologi AI

Kasus ini juga menyoroti berbagai tantangan dalam penegakan hukum terhadap kejahatan digital berbasis AI.

Pertama, keterbatasan regulasi menjadi masalah utama. UU ITE belum secara khusus mengatur penggunaan kecerdasan buatan atau pemalsuan digital seperti deepfake. Akibatnya, aparat penegak hukum sering kali menggunakan pasal umum yang tidak selalu mencerminkan kompleksitas teknologi yang digunakan pelaku.

Kedua, pembuktian digital (digital forensics) menjadi tantangan tersendiri. Video deepfake memiliki tingkat realisme tinggi sehingga memerlukan perangkat lunak forensik canggih untuk mendeteksi manipulasi. Dalam kasus ini, Polri menggunakan dua software pendeteksi deepfake yang menunjukkan skor 1.00 indikasi 100% palsu, namun tidak semua lembaga penegak hukum memiliki kemampuan teknis setara.

Ketiga, penanganan konten lintas platform juga menjadi kendala. Video deepfake tidak hanya diunggah di Instagram, tetapi juga disebarluaskan melalui TikTok dan platform lain, sehingga proses takedown memerlukan koordinasi dengan perusahaan teknologi internasional yang sering memakan waktu.

Keempat, rendahnya literasi digital masyarakat menjadi faktor yang memperburuk situasi. Banyak korban tidak memahami bahwa teknologi dapat menciptakan video palsu yang sangat meyakinkan. Akibatnya, mereka mudah percaya pada konten yang meniru tokoh publik dan akhirnya terjebak dalam penipuan.

4. Arah Penguatan dan Pembaruan Regulasi

Melihat kompleksitas kejahatan berbasis AI, Indonesia perlu segera memperkuat sistem hukum agar lebih adaptif terhadap perkembangan teknologi. Beberapa langkah strategis yang dapat dilakukan antara lain[17]:

1) Penyusunan regulasi khusus mengenai AI dan deepfake, baik dalam bentuk revisi UU ITE maupun peraturan turunan yang menegaskan batas etika dan tanggung jawab hukum bagi pengguna teknologi AI.
2) Peningkatan kapasitas aparat penegak hukum dalam bidang digital forensik, agar mampu menganalisis bukti berbasis AI dengan cepat dan akurat.
3) Kerja sama dengan platform digital internasional, seperti Meta dan TikTok, untuk mendeteksi dan menghapus konten deepfake secara otomatis.
4) Pendidikan hukum dan literasi digital publik, agar masyarakat lebih waspada dan kritis terhadap konten yang beredar di media sosial.

Dengan pembaruan regulasi dan peningkatan kapasitas hukum, Indonesia dapat memperkuat perlindungan masyarakat dari kejahatan berbasis kecerdasan buatan. Kasus deepfake yang mencatut nama Presiden Prabowo Subianto menunjukkan bahwa hukum pidana Indonesia masih mampu menjerat pelaku meskipun belum ada regulasi khusus tentang AI. Namun, tantangan teknologis dan pembuktian digital menuntut sistem hukum yang lebih adaptif. Penegakan hukum perlu disertai pembaruan regulasi, kolaborasi lintas lembaga, dan edukasi publik untuk mencegah penyalahgunaan teknologi di masa depan. Dengan demikian, penanganan

[17] Madalaine Christella Seveney, Demas Brian Wicaksono, dan Irwan Kurniawan Soetijono, "Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi," *Disiplin : Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda* 31, no. 2 (Mei 2025): 97–106, https://doi.org/10.46839/disiplin.v31i2.1167.

kasus deepfake tidak hanya menjadi upaya represif, tetapi juga langkah preventif dalam membangun ekosistem digital yang aman, etis, dan berkeadilan[18].

e. Dampak Sosial dan Komunikatif Penyebaran Video Deepfake

Fenomena penyebaran video deepfake di Indonesia, khususnya kasus yang mencatut nama Presiden Prabowo Subianto pada tahun 2025, tidak hanya menimbulkan kerugian ekonomi bagi masyarakat, tetapi juga mengakibatkan dampak sosial dan komunikatif yang signifikan. Deepfake tidak sekadar menjadi alat penipuan digital, tetapi juga simbol bagaimana teknologi dapat mengubah cara masyarakat menerima, mempercayai, dan menyebarkan informasi. Dalam konteks komunikasi modern, kemunculan video palsu berbasis kecerdasan buatan (Artificial Intelligence/AI) ini menjadi ancaman terhadap keutuhan informasi publik dan stabilitas sosial[19].

1. Dampak terhadap Kepercayaan Publik

Salah satu dampak paling serius dari penyebaran video deepfake adalah menurunnya kepercayaan publik terhadap pemerintah dan tokoh masyarakat. Video yang menampilkan Presiden Prabowo seolah-olah sedang berbicara tentang bantuan sosial membuat masyarakat sulit membedakan antara kenyataan dan rekayasa. Ketika video palsu tampak begitu autentik, publik cenderung percaya tanpa melakukan verifikasi.

Kondisi ini menimbulkan krisis kepercayaan terhadap komunikasi resmi pemerintah. Banyak masyarakat mulai meragukan keaslian pernyataan pejabat negara yang beredar di media sosial, karena takut tertipu oleh rekayasa visual. Akibatnya, reputasi lembaga negara pun dapat tergerus karena persepsi negatif publik yang dibentuk oleh informasi palsu. Dalam jangka panjang, hal ini berpotensi mengganggu legitimasi politik dan kepercayaan terhadap otoritas publik, terutama jika tidak ada penanganan hukum dan klarifikasi yang cepat.

2. Dampak Sosial dan Ekonomi bagi Masyarakat

Selain menggerus kepercayaan, kasus deepfake juga menimbulkan kerugian sosial dan ekonomi yang luas. Berdasarkan data dari Bareskrim Polri, lebih dari 100 korban dari 20 provinsi menjadi sasaran penipuan dengan total kerugian mencapai sekitar Rp65 juta. Sebagian besar korban berasal dari lapisan masyarakat dengan tingkat literasi digital rendah, terutama di daerah pedesaan dan kelompok usia lanjut. Bagi mereka, video deepfake yang menampilkan sosok Presiden dianggap sebagai bentuk komunikasi langsung dari pemerintah. Ketika iming-iming bantuan disertai permintaan biaya administrasi kecil, banyak yang tergoda karena faktor kebutuhan ekonomi. Setelah menyadari bahwa video tersebut palsu, korban tidak hanya kehilangan uang, tetapi juga mengalami trauma sosial dan rasa malu karena merasa tertipu.

Fenomena ini memperlihatkan adanya ketimpangan literasi digital di masyarakat. Di satu sisi, teknologi semakin canggih dan mudah diakses, namun di sisi lain, pemahaman masyarakat terhadap teknologi masih terbatas. Akibatnya, masyarakat menjadi sasaran empuk bagi kejahatan digital yang memanfaatkan kepercayaan dan ketidaktahuan publik[20].

3. Dampak terhadap Komunikasi Publik dan Disinformasi

Dari perspektif komunikasi, penyebaran video deepfake menciptakan disrupsi informasi (*information disorder*) yang berbahaya. Dalam teori komunikasi massa, salah satu fondasi penting kepercayaan publik adalah kredibilitas sumber. Namun, deepfake

[18] Lukman Satria Manggala, Mulia Rahmayu, dan Mia Rosmiati, "Analisis Pengaruh Penggunaan Deepfake Di Masyarakat Dengan Metode Technology Acceptance Model," *Jurnal Komputer Teknologi Informasi Sistem Komputer (JUKTISI)* 4, no. 2 (September 2025): 1282–87, https://doi.org/10.62712/juktisi.v4i2.609.

[19] Muslim Nugraha dkk., "Analisis Unsur Perbuatan Melanggar Hukum Atas Penggunaan Artificial Intelligence Dalam Kasus Konten Deepfake," *Legal System Journal* 2, no. 1 (Juni 2025): 23–36, https://doi.org/10.70656/lsj.v2i1.392.

[20] Muhammad Hanan Nuhi dkk., "Pembaharuan Hukum Penanganan Tindak Pidana Pemalsuan Identitas Akibat Penyalahgunaan Artificial Intelligence Di Indonesia," *Jurnal Batavia* 1, no. 2 (2024): 80–88.

telah mengaburkan batas antara realitas dan manipulasi digital. Ketika wajah dan suara seseorang dapat direkayasa secara sempurna, masyarakat kehilangan kemampuan membedakan mana pesan otentik dan mana yang palsu.

Hal ini memicu disinformasi dan chaos komunikatif, di mana setiap individu memiliki potensi untuk menjadi penyebar hoaks tanpa disadari. Dalam kasus Prabowo, video palsu tidak hanya beredar di Instagram, tetapi juga di TikTok, Facebook, dan WhatsApp, dengan jutaan tayangan dan ribuan komentar. Pola penyebaran semacam ini menunjukkan bagaimana algoritma media sosial memperkuat pesan manipulatif karena sifatnya yang sensasional dan mudah viral.

Dampak komunikatif lainnya adalah munculnya krisis otentisitas pesan. Masyarakat mulai mempertanyakan validitas setiap konten digital, termasuk berita, video kampanye, hingga pidato resmi. Bila kondisi ini berlanjut tanpa edukasi digital yang memadai, publik dapat mengalami keletihan informasi (*information fatigue*) dan menjadi apatis terhadap komunikasi politik dan pemerintahan.

4. Dampak terhadap Psikologi dan Interaksi Sosial

Video deepfake juga menimbulkan dampak psikologis yang tidak kalah besar. Korban penipuan mengalami rasa cemas, marah, dan kehilangan kepercayaan diri karena merasa mudah dikelabui. Dalam beberapa kasus, korban bahkan menjadi enggan berinteraksi dengan media digital karena trauma.

Selain itu, fenomena deepfake memperparah polarisasi sosial. Di media sosial, perdebatan sering kali muncul antara pihak yang percaya dan yang tidak percaya terhadap kebenaran video. Diskusi publik menjadi tidak sehat karena dipenuhi tuduhan, spekulasi, dan narasi politik yang menyesatkan. Kondisi ini memperlihatkan bahwa deepfake tidak hanya menyerang individu, tetapi juga merusak kualitas komunikasi sosial dan memperlebar jurang disinformasi di masyarakat.

5. Upaya Mengurangi Dampak Sosial dan Komunikatif

Untuk meminimalisir dampak sosial dan komunikatif dari penyebaran video deepfake, diperlukan langkah strategis dari berbagai pihak. Pemerintah harus meningkatkan literasi digital nasional, terutama dalam mengenali konten manipulatif berbasis AI. Kampanye publik tentang bahaya deepfake perlu diperluas hingga ke daerah-daerah terpencil melalui kerja sama antara Kementerian Komunikasi dan Digital (Kemenkom Digi), lembaga pendidikan, serta komunitas masyarakat. Selain itu, platform media sosial juga memiliki tanggung jawab etis dan hukum untuk mengembangkan sistem deteksi otomatis terhadap konten deepfake. Teknologi berbasis AI forensics dapat digunakan untuk mendeteksi manipulasi wajah dan suara sebelum konten dipublikasikan. Langkah preventif ini penting agar masyarakat tidak terus-menerus terpapar hoaks yang dapat memicu keresahan sosial.

Penyebaran video deepfake bukan sekadar masalah teknologi, tetapi persoalan sosial dan komunikasi yang kompleks. Ia mengubah pola kepercayaan, memperburuk disinformasi, dan menimbulkan kerugian nyata bagi masyarakat. Kasus deepfake yang mencatut nama Presiden Prabowo menjadi peringatan bahwa kemajuan AI harus diimbangi dengan etika, regulasi, dan literasi digital yang kuat. Jika tidak, masyarakat akan terus hidup dalam era kebingungan informasi, di mana kebenaran dan kebohongan sulit dibedakan[21].

f. Upaya Penanggulangan dan Pencegahan

Fenomena penyalahgunaan teknologi deepfake di Indonesia, seperti dalam kasus yang mencatut nama Presiden Prabowo Subianto pada tahun 2025, menunjukkan bahwa kejahatan digital berbasis Artificial Intelligence (AI) telah menjadi tantangan baru bagi sistem hukum, keamanan siber, dan tatanan sosial. Upaya penanggulangan dan

[21] Mu, Adrezo, dan Haikal, "Identifikasi Wajah Asli Dan Buatan Deepfake Menggunakan Metode Convolutional Neural Network."

pencegahan tidak dapat dilakukan secara parsial, melainkan harus melibatkan kolaborasi antara pemerintah, aparat penegak hukum, lembaga pendidikan, platform digital, serta masyarakat. Tujuannya adalah menciptakan ekosistem digital yang aman, beretika, dan adaptif terhadap perkembangan teknologi[22].

1. Penegakan Hukum dan Penguatan Kapasitas Aparat Siber

Langkah pertama yang paling mendasar dalam menanggulangi kejahatan deepfake adalah penegakan hukum yang tegas dan efektif. Aparat penegak hukum, khususnya Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri, telah melakukan sejumlah tindakan penting, seperti patroli siber, pengungkapan kasus, dan penangkapan pelaku. Dalam kasus deepfake Prabowo, keberhasilan polisi menangkap dua pelaku (AMA dan JS) menunjukkan komitmen aparat dalam menindak pelanggaran digital. Namun, di sisi lain, tantangan yang dihadapi cukup besar. Proses identifikasi, pembuktian digital, dan pelacakan akun sering kali memerlukan kemampuan teknis tinggi. Oleh karena itu, peningkatan kapasitas sumber daya manusia di bidang digital forensik dan analisis AI menjadi prioritas. Aparat penegak hukum perlu dilatih untuk memahami cara kerja teknologi deepfake, mengenali pola manipulasi berbasis Generative Adversarial Network (GAN), serta menggunakan perangkat lunak deteksi otomatis.

Selain itu, diperlukan kerja sama internasional karena banyak platform media sosial yang berbasis di luar negeri. Kolaborasi dengan perusahaan teknologi global seperti Meta, TikTok, dan Google sangat penting untuk mempercepat proses takedown konten deepfake serta melacak asal pembuatan video palsu.

2. Pembaruan Regulasi dan Kebijakan Pemerintah

Perkembangan teknologi AI berjalan jauh lebih cepat dibanding pembaruan hukum di Indonesia. Oleh karena itu, pemerintah perlu menyusun regulasi khusus yang mengatur penggunaan dan penyalahgunaan AI, termasuk deepfake. Selama ini, penegakan hukum masih mengandalkan UU ITE dan KUHP yang belum sepenuhnya menjangkau kompleksitas kejahatan digital modern.

Regulasi baru sebaiknya mencakup beberapa aspek penting[23]:

1) Batas etika dan tanggung jawab pengguna AI, baik individu maupun korporasi.
2) Klasifikasi konten berbasis AI yang mengandung potensi manipulatif, agar masyarakat dapat dengan mudah mengenali label "konten buatan AI."
3) Kewajiban platform digital untuk memiliki sistem deteksi deepfake internal serta prosedur pelaporan publik yang cepat.
4) Perlindungan terhadap data wajah dan suara publik agar tidak disalahgunakan untuk pembuatan konten palsu.

Selain itu, Indonesia dapat mencontoh kebijakan dari Uni Eropa melalui European AI Act, yang menetapkan prinsip kehati-hatian, transparansi, dan tanggung jawab dalam pengembangan serta distribusi teknologi AI. Pendekatan serupa dapat diadaptasi untuk melindungi masyarakat Indonesia dari penyalahgunaan teknologi.

3. Literasi Digital dan Edukasi Publik

Pencegahan kejahatan deepfake tidak dapat sepenuhnya bergantung pada aparat penegak hukum. Peran masyarakat sangat penting melalui peningkatan literasi digital. Banyak korban penipuan deepfake berasal dari kalangan dengan tingkat pemahaman teknologi yang rendah. Oleh karena itu, edukasi publik menjadi kunci utama dalam pencegahan.

Program literasi digital perlu difokuskan pada tiga aspek[24]:

[22] Nugraha dkk., "Analisis Unsur Perbuatan Melanggar Hukum Atas Penggunaan Artificial Intelligence Dalam Kasus Konten Deepfake."

[23] Muhammad Syafiq Wafi, Aloysius Wisnubroto, dan Yudi Prayudi, "Artificial Intelligence-Based Deepfake Crimes: A Conception of Culpability Principle as a Criminal Liability Reform," *Reformasi Hukum* 29, no. 2 (2025): 168–83.

[24] Angelica Vanessa Audrey Nasution, Suteki Suteki, dan Anggita Doramia Lumbanraja, "Prospek Pemenuhan Right to Be Forgotten (RTBF) Bagi Korban Deepfake Pornography Akibat Penyalahgunaan

1) Kemampuan mengenali konten manipulatif

Masyarakat harus diberi pemahaman tentang ciri-ciri video deepfake, seperti pergerakan wajah yang tidak natural, sinkronisasi bibir yang tidak sempurna, atau pencahayaan yang tidak konsisten.

2) Kebiasaan verifikasi informasi

Setiap informasi yang mengatasnamakan pejabat negara atau institusi resmi harus dicek melalui kanal resmi pemerintah sebelum dibagikan atau dipercaya.

3) Kesadaran privasi digital

Pengguna internet harus memahami pentingnya menjaga data pribadi, termasuk foto dan video, agar tidak disalahgunakan oleh pihak lain.

Pemerintah, melalui Kementerian Komunikasi dan Digital (Kemenkom Digi), dapat menggandeng lembaga pendidikan, komunitas masyarakat, dan media untuk menyelenggarakan kampanye nasional bertema "Cerdas Digital, Lawan Deepfake." Kampanye semacam ini akan membentuk pola pikir kritis masyarakat terhadap konten digital yang beredar[25].

4. Inovasi Teknologi dan Deteksi Otomatis

Selain pendekatan hukum dan edukatif, upaya teknologis juga sangat penting. Pemerintah bersama sektor swasta perlu berinvestasi dalam teknologi pendeteksi deepfake (AI Forensics). Sistem ini menggunakan algoritma pembelajaran mesin untuk menganalisis kejanggalan visual dan audio pada video, seperti pola piksel yang tidak wajar atau perbedaan ritme suara. Beberapa universitas dan lembaga riset di Indonesia juga dapat berperan dalam mengembangkan algoritma pendeteksi lokal yang disesuaikan dengan konteks bahasa dan wajah tokoh nasional. Teknologi ini tidak hanya berguna untuk kepentingan hukum, tetapi juga untuk melindungi integritas komunikasi publik. Selain itu, platform media sosial harus menerapkan labelisasi konten berbasis AI, yaitu tanda khusus yang menunjukkan bahwa suatu video dihasilkan atau dimodifikasi menggunakan kecerdasan buatan. Label ini membantu pengguna mengenali konten non-otentik sejak awal sebelum mempercayainya.

5. Kolaborasi Multi-Stakeholder

Kejahatan berbasis deepfake bersifat lintas sektor dan lintas batas. Oleh karena itu, kolaborasi antara pemerintah, sektor swasta, akademisi, media, dan masyarakat sipil sangat diperlukan. Pemerintah dapat berperan sebagai regulator, akademisi sebagai penyedia riset dan teknologi, sedangkan media dan komunitas menjadi perantara edukasi kepada publik. Kolaborasi internasional juga penting, karena penyebaran deepfake tidak mengenal batas negara. Indonesia perlu bergabung dalam forum kerja sama global mengenai AI ethics dan cyber law, agar dapat berbagi pengalaman dan strategi penegakan hukum dengan negara lain.

Kasus deepfake yang mencatut nama Presiden Prabowo Subianto harus dijadikan momentum untuk memperkuat kesadaran nasional tentang pentingnya keamanan digital. Dengan sinergi antarinstansi dan masyarakat, Indonesia dapat menghadapi era kecerdasan buatan dengan lebih bijak, melindungi ruang publik dari manipulasi digital, dan menjaga kepercayaan terhadap kebenaran informasi di tengah arus teknologi yang terus berkembang[26].

4. Kesimpulan

Kasus video deepfake yang mencatut nama Presiden Prabowo Subianto pada tahun 2025 menunjukkan bagaimana kemajuan teknologi *Artificial Intelligence (AI)* dapat dimanfaatkan secara destruktif untuk tujuan penipuan dan disinformasi. Deepfake, sebagai produk dari teknologi Generative Adversarial Network (GAN), mampu menciptakan konten visual dan audio yang sangat realistis hingga sulit dibedakan dari yang asli. Akibatnya, masyarakat menjadi rentan terhadap manipulasi digital yang mengatasnamakan

Artificial Intelligence (AI) Di Indonesia" (other, Fakultas Hukum Universitas Diponegoro, 2024), https://eprints2.undip.ac.id/id/eprint/22578/.

[25] Nadiyah, Winarno, dan Ariesta, "Kajian Hukum Terhadap Penggunaan Artificial Intelligence (AI) Yang Berakibat Menyerang Kehormatan."

[26] Manggala, Rahmayu, dan Rosmiati, "Analisis Pengaruh Penggunaan Deepfake Di Masyarakat Dengan Metode Technology Acceptance Model."

pejabat publik atau institusi pemerintah. Dari sisi hukum, tindakan pelaku telah memenuhi unsur tindak pidana sebagaimana diatur dalam Pasal 35 Jo Pasal 51 ayat (1) UU ITE dan Pasal 378 KUHP tentang penipuan. Namun, kasus ini juga menegaskan perlunya regulasi khusus yang mengatur penggunaan dan penyalahgunaan AI, karena hukum yang ada belum sepenuhnya mampu menjangkau kompleksitas kejahatan berbasis teknologi. Dampak sosial yang timbul meliputi menurunnya kepercayaan publik terhadap pemerintah, meningkatnya kerentanan terhadap hoaks, serta kerugian ekonomi dan psikologis bagi masyarakat. Oleh karena itu, upaya penanggulangan tidak dapat berhenti pada penegakan hukum semata, tetapi harus diimbangi dengan edukasi literasi digital, penguatan kemampuan forensik siber, dan kerja sama lintas sektor.

References

Darmawan, Muh Taufik, Amir Junaidi, dan Ariy Khaerudin. "Penegakan Hukum Terhadap Penyalahgunaan Deepfake Pada Pornografi Anak Di Era Artifical Intelegence di Indonesia." *Jurnal Penelitian Serambi Hukum* 18, no. 01 (Januari 2025): 42–54. https://doi.org/10.59582/sh.v18i01.1257.

Fadhilah, Almira Daisy Zahrah, dan Sri Retnoningsih. "Perancangan Kampanye Digital Melawan Disinformasi Melalui Artificial Intelligence Dan Deepfake Di Kalangan Pra Lansia Usia 45-55 Tahun." *FAD* 3, no. 02 (Juli 2024). https://eproceeding.itenas.ac.id/index.php/fad/article/view/2943.

Hidayat, Muhammad Nur. "Pertanggungjawaban Pidana Terhadap Penyalahgunaan Deepfake Sebagai Ancaman Keamanan Data Pribadi." *UNES Law Review* 7, no. 4 (Juli 2025): 2036–48. https://doi.org/10.31933/unesrev.v7i4.2433.

Luxiana, Kadek Melda. "Bareskrim Limpahkan Berkas 2 Tersangka Deepfake Catut Prabowo ke Kejaksaan." Detiknews, 2025. https://news.detik.com/berita/d-7883615/bareskrim-limpahkan-berkas-2-tersangka-deepfake-catut-prabowo-ke-kejaksaan.

Maharani, Rambu, dan Sri Maharani M.t.v.m. "Ganti Rugi Akibat Penyalahgunaan Artificial Intelligence (Deepfake) pada Citra Orang Terkenal di Facebook Berdasarkan Pasal 1365 BW." *Jurnal Hukum Lex Generalis* 6, no. 4 (April 2025). https://doi.org/10.56370/jhlg.v6i4.1512.

Manggala, Lukman Satria, Mulia Rahmayu, dan Mia Rosmiati. "Analisis Pengaruh Penggunaan Deepfake Di Masyarakat Dengan Metode Technology Acceptance Model." *Jurnal Komputer Teknologi Informasi Sistem Komputer (JUKTISI)* 4, no. 2 (September 2025): 1282–87. https://doi.org/10.62712/juktisi.v4i2.609.

Maria Karunia Putri Maan, Heryanto Amalo, dan Ngongo Dede. "Analisis Perlindungan Hukum terhadap Penyimpangan Artificial Intelligence dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana." *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora* 4, no. 1 (Januari 2025): 296–307. https://doi.org/10.55606/jurrish.v4i1.5071.

Mu, Jesselyn, Muhammad Adrezo, dan Ahmed Nizhan Haikal. "Identifikasi Wajah Asli Dan Buatan Deepfake Menggunakan Metode Convolutional Neural Network." *Teknika* 13, no. 1 (Januari 2024): 45–50. https://doi.org/10.34148/teknika.v13i1.705.

Nadiyah, Nadiyah, Ronny Winarno, dan Wiwin Ariesta. "Kajian Hukum Terhadap Penggunaan Artificial Intelligence (AI) Yang Berakibat Menyerang Kehormatan." *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory* 3, no. 3

(Juli 2025): 2415–22. https://doi.org/10.62976/ijijel.v3i3.1287.

Nasution, Angelica Vanessa Audrey, Suteki Suteki, dan Anggita Doramia Lumbanraja. "Prospek Pemenuhan Right to Be Forgotten (RTBF) Bagi Korban Deepfake Pornography Akibat Penyalahgunaan Artificial Intelligence (AI) Di Indonesia." Other, Fakultas Hukum Universitas Diponegoro, 2024. https://eprints2.undip.ac.id/id/eprint/22578/.

Nugraha, Muslim, Amanda Sela Sadina, Viraliza Ramadonna, dan Keysyah Aulia Hidayat. "Analisis Unsur Perbuatan Melanggar Hukum Atas Penggunaan Artificial Intelligence Dalam Kasus Konten Deepfake." *Legal System Journal* 2, no. 1 (Juni 2025): 23–36. https://doi.org/10.70656/lsj.v2i1.392.

Nuhi, Muhammad Hanan, Logan Al Ghozi, Syakira Nazla, dan Davina Syakirah. "Pembaharuan Hukum Penanganan Tindak Pidana Pemalsuan Identitas Akibat Penyalahgunaan Artificial Intelligence Di Indonesia." *Jurnal Batavia* 1, no. 2 (2024): 80–88.

Rahman, AUNF, Syariffudin Syariffudin, dan Fathol Bari. "Perlindungan Hukum terhadap Korban Penyalahgunaan Teknik Deepfake." *Jurnal Perspektif Administrasi Publik dan Hukum* 2 (2025): 247–55.

Respati, Adnasohn Aqilla. "Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation." *Jurnal USM Law Review* 7, no. 3 (Desember 2024): 1737–58. https://doi.org/10.26623/julr.v7i3.10578.

Seveney, Madalaine Christella, Demas Brian Wicaksono, dan Irwan Kurniawan Soetijono. "Urgensi Regulasi Terhadap Penyalahgunaan Deepfake Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi." *Disiplin : Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda* 31, no. 2 (Mei 2025): 97–106. https://doi.org/10.46839/disiplin.v31i2.1167.

Syahirah, Sabrina Nur, dan Bayu Prasetyo. "Tinjauan Yuridis Terhadap Penggunaan Teknologi Deepfake Untuk Pornografi Melalui Artificial Intelligence (AI) Di Indonesia." *Jurnal Inovasi Hukum Dan Kebijakan* 6, no. 1 (2025).

Wafi, Muhammad Syafiq, Aloysius Wisnubroto, dan Yudi Prayudi. "Artificial Intelligence-Based Deepfake Crimes: A Conception of Culpability Principle as a Criminal Liability Reform." *Reformasi Hukum* 29, no. 2 (2025): 168–83.

Wirakusunah, Gelar. "Pengembangan Media Pembelajaran Pengenalan Sejarah Pahlawan Indonesia Menggunakan Deep Fake Dengan Metode Multimedia Development Life Cycle." *Jurnal Informatika Dan Teknik Elektro Terapan* 12, no. 2 (April 2024). https://doi.org/10.23960/jitet.v12i2.4171.