



Analisis Penyalahgunaan Teknologi *Deepfake* dalam Penyebaran Hoaks Digital

Janeta Tefa¹, Arief Riful Haq², Wijaya Guruh³, Bimo Febriyanto⁴, Annisa Elfina Augustia⁵

^{1,2,3,4,5}Fakultas Teknik dan Ilmu Komputer, Teknik Informatika, Universitas Indraprasta PGRI, DKI Jakarta, Jakarta Timur, Indonesia

Email: ¹janetaputra09@gmail.com, ²ariefdrh45@gmail.com, ³wijayaguruh@gmail.com,
⁴bimofbrynt7@gmail.com, ⁵annisa12elfina@gmail.com
(*: coresponding author)

Abstrak—Kemajuan teknologi telah menggeser pandangan manusia tentang betapa mudahnya mengatasi berbagai tantangan dunia yang kompleks. Perkembangan ini memberikan banyak keuntungan signifikan, seperti mempermudah pencarian data dan sarana komunikasi yang tak terbatas oleh jarak geografis. Namun, di balik itu, muncul masalah akibat penyalahgunaan teknologi untuk tujuan pribadi semata, salah satunya adalah *deepfake*. Penelitian ini bertujuan mengurangi risiko dari teknologi *deepfake* dengan sudut pandang literasi digital. Pendekatan yang dipakai adalah metode kualitatif, dengan pengumpulan data melalui kajian literatur. Temuan utamanya menunjukkan bahwa *deepfake* merupakan inovasi kecerdasan buatan (AI) yang dimanfaatkan untuk mengubah gambar atau video demi kepentingan spesifik, contohnya untuk menciptakan dan menyebarkan berita palsu atau hoaks di tengah masyarakat. Kesimpulannya, langkah pencegahan efektif adalah dengan memperkuat pemahaman literasi digital. Melalui kemampuan ini, orang bisa lebih baik dalam mengakses, menyaring, memilih, dan memahami berbagai macam informasi, yang pada akhirnya bisa meningkatkan kualitas hidup dan lingkungan sekitar. Untuk itu, dibutuhkan regulasi yang lebih tegas dan fleksibel, kolaborasi erat antara pemerintah serta platform online, plus upaya intensif meningkatkan literasi digital masyarakat guna meminimalkan bahaya kejahatan *deepfake* di dunia maya.

Kata Kunci: Teknologi *Deepfake*; Hoaks Digital; Literasi Digital; Kecerdasan Buatan; Keamanan Siber

Abstract—Technological advancements have shifted humanity's perspective on how easily we can overcome the complex challenges of the world. This development offers many significant advantages, such as making data retrieval easier and providing communication tools that are not limited by geographical distance. However, behind that, problems arise from the misuse of technology for purely personal purposes, one of which is *deepfakes*. This research aims to reduce the risks of *deepfake* technology from a digital literacy perspective. The approach used is a qualitative method, with data collection thru literature review. The main findings indicate that *deepfakes* are an artificial intelligence (AI) innovation used to alter images or videos for specific purposes, such as creating and spreading fake news or hoaxes within society. In conclusion, an effective preventive measure is to strengthen digital literacy understanding. Thru this ability, people can become better at accessing, filtering, selecting, and understanding a wide variety of information, which can ultimately improve their quality of life and the surrounding environment. Therefore, stricter and more flexible regulations are needed, along with close collaboration between the government and online platforms, and intensive efforts to improve public digital literacy in order to minimize the dangers of *deepfake* crimes in cyberspace.

Keywords: *Deepfake* Tecnology; Digital Hoax; Digital Literacy; Artificial Intelligence; Cybersecurity

1. PENDAHULUAN

Perkembangan *Artificial Intelligence* (AI) selama dekade terakhir telah menciptakan inovasi-inovasi yang memberikan manfaat substansial di berbagai bidang. Namun, kemajuan ini juga menimbulkan bentuk kejahatan digital yang semakin rumit, termasuk penyalahgunaan teknologi *deepfake*. Teknologi ini didefinisikan sebagai hasil rekayasa visual dan audio yang didasarkan pada machine learning, yang memungkinkan pengubahan wajah atau suara seseorang dengan tingkat keakuratan tinggi (Kietzmann et al., 2020). Di Indonesia, fenomena tersebut semakin memprihatinkan karena dimanfaatkan untuk menyebarkan hoaks, melakukan penipuan digital, propaganda politik, dan manipulasi opini publik. Laporan dari Kementerian Komunikasi dan Informatika (Kominfo, 2024) menunjukkan bahwa lebih dari 11.000 kasus hoaks digital telah terdeteksi dalam tiga tahun terakhir, dengan peningkatan signifikan pada konten manipulatif yang berbasis AI.



JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2127-2131

Penyalahgunaan teknologi deepfake tidak hanya memengaruhi aspek sosial dan psikologis, tetapi juga mengancam keamanan informasi, kredibilitas pejabat publik, serta stabilitas politik nasional. Sebagai contoh, video manipulatif yang meniru tokoh negara sering digunakan dalam modus penipuan bantuan sosial, yang mengakibatkan kerugian finansial dan emosional bagi korban. Penelitian Utsalina (2017) menjelaskan bahwa penyebaran hoaks menjadi sangat efektif apabila melibatkan figur otoritatif dan sentimen publik. Sementara itu, Park (2013) menyatakan bahwa kecepatan distribusi informasi digital tanpa verifikasi memperbesar dampak disinformasi secara masif. Dalam konteks Indonesia, lemahnya literasi digital dan absennya regulasi spesifik terkait deepfake memperburuk penyebaran konten palsu.

Upaya mencegah penyebaran hoaks yang disebabkan oleh teknologi deepfake dapat dilakukan dengan meningkatkan literasi digital atau literasi teknologi di tengah masyarakat. Syah et al. (2019) mengartikan literasi digital sebagai kemampuan seseorang untuk menyampaikan, menilai, dan menemukan fakta dari berbagai sumber digital. Menyoroti pentingnya literasi digital dalam bidang komunikasi dan informasi masyarakat, terutama dengan meningkatnya penggunaan media digital seperti internet dan media sosial, ketergantungan besar pada teknologi dan platform digital, serta perlunya menyaring informasi yang beredar. Dengan demikian, literasi digital perlu didorong sebagai langkah pencegahan terhadap masalah penyebaran berita palsu (hoaks) yang diperparah oleh perkembangan teknologi deepfake saat ini dan di masa mendatang. Penelitian ini diharapkan memberikan manfaat praktis bagi masyarakat sehingga mereka dapat mengenali deepfake di era digital (Nisa, 2024).

Dengan demikian, penelitian ini tidak hanya memberikan kontribusi pada kajian akademik, tetapi juga menawarkan implikasi praktis sebagai dasar pengembangan literasi digital, regulasi adaptif, dan strategi mitigasi terhadap penyebaran hoaks berbasis deepfake. Analisis ini menjadi penting mengingat ancaman ke depan tidak hanya berasal dari produksi informasi palsu manual, tetapi dari teknologi manipulatif tingkat lanjut yang sulit dibedakan secara kasat mata.

2. METODE

Metode ini menggunakan penelitian kualitatif. Menurut Harahap (2020), penelitian kualitatif, juga dikenal sebagai penelitian alamiah, berfokus pada proses yang tidak diperiksa atau dievaluasi ketika menggunakan data deskriptif. Berbagai teknik pengumpulan data digunakan dalam penelitian kualitatif, salah satunya adalah studi atau analisis literatur. Kajian literatur dalam penelitian kualitatif mendorong peneliti untuk mencari dan menganalisis suatu fenomena secara cermat, hati-hati, dan kritis, dengan mencari fakta melalui analisis jurnal dan artikel, kemudian melakukan analisis hasil. Untuk alasan ini, dalam penelitian ini, peneliti menggunakan penelitian kualitatif, yaitu tinjauan pustaka, untuk mengumpulkan informasi tentang fenomena yang ada.

3. ANALISA DAN PEMBAHASAN

3.1 Kemunculan Teknologi Deepfake

Menurut publikasi *A Shallow History of Deepfakes* (2025), cikal bakal teknologi ini bisa ditelusuri sejak 1997, ketika tiga ilmuwan komputer – Christoph Bregler, Michele Covell, dan Malcolm Slaney – memperkenalkan perangkat lunak *Video Rewrite. Software* ini mampu memanfaatkan rekaman asli untuk menciptakan video baru, sehingga seseorang tampak mengucapkan kata-kata yang tidak pernah diucapkan sebelumnya. Prinsip kerjanya adalah memetakan gerakan bibir, gigi, dan rahang berdasarkan data suara, lalu menyesuaikannya di dalam video. Awalnya, teknologi ini digunakan untuk dubbing film, telekonferensi, dan efek khusus. Inspirasi para ilmuwan datang dari film *Forrest Gump* (1994) yang menampilkan adegan Presiden John F. Kennedy dan Richard Nixon seolah-olah berbicara melalui efek digital.

Perkembangan machine learning dan kecerdasan buatan (AI) mengubah dunia pada awal tahun 2010-an. Pengenalan *Generative Adversarial Networks* (GANs) oleh Ian Goodfellow pada tahun 2014 adalah salah satu kemajuan terbesar. Algoritma yang dikenal sebagai GANs memungkinkan komputer untuk mempelajari pola data dan membuat konten baru yang sangat realistis. Konsep ini membentuk dasar teknologi deepfake, memungkinkan gambar, video, dan audio palsu yang hampir tidak dapat dibedakan dari yang sebenarnya.



JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2127-2131

Istilah "deepfake" pertama kali muncul di platform diskusi internet Reddit sekitar tahun 2017. Seorang pengguna anonim yang dikenal sebagai "Deepfakes" mulai memposting video manipulasi yang menggunakan teknologi deep learning untuk menukar wajah selebritas dengan tubuh orang lain, sering kali dalam konteks yang jelas. Video-video ini menjadi viral, membuat publik kagum dan ketakutan. Kehadiran deepfake di Reddit menunjukkan betapa cepatnya teknologi ini berkembang. Perangkat lunak dan alat yang digunakan untuk membuat deepfake menjadi lebih mudah diakses oleh publik dalam waktu singkat. (Saiyad Mahmmadakram Hanif & Vivek Dave, 2022)

FakeApp, yang juga disebut sebagai aplikasi tiruan, merupakan program komputer yang dimanfaatkan untuk mengganti wajah satu individu dengan wajah orang lain. Aplikasi semacam ini membutuhkan banyak data untuk menghasilkan data yang bagus. Sistem akan menerima data ini dan memproses model wajah target. Penciptaan wajah palsu ini memerlukan ekstraksi gambar dan video untuk membuat gambar atau video palsu yang sempurna. Berikutnya adalah teknik offsite ekspresi dinamis (DDE). Ini adalah teknik dengan ketelitian tinggi yang menggunakan waktu dan sistem dan memungkinkan desain lebih rinci.

Generasi deepfake berikutnya mencakup pendekatan pelacakan yang menggunakan model wajah berbasis parameter. Dalam proses pelacakan model tersebut, pencahayaan diterapkan di sekitar area mulut, yang mencakup proksi gigi dan bagian dalam mulut. Metode sebelumnya dinilai kurang efektif. Teknik ini menghasilkan gambar yang sangat detail dengan menerapkan Teknik RGB-D, yang memungkinkan perhalusan ekspresi aktor dan produksi gambar yang lebih akurat. Berdasarkan paparan tersebut, kemajuan teknologi informasi dan kecerdasan buatan, yang juga dikenal sebagai AI, yang begitu pesat, pasti akan menimbulkan masalah yang sangat signifikan. Hal ini disebabkan oleh kenyataan bahwa hampir semua lembaga, termasuk pemerintah, perusahaan, dan organisasi sipil, mengandalkan sistem informasi digital, sehingga membuatnya rentan terhadap ancaman.

3.2 Kemunculan Permasalahan Deepfake

Masalah penggunaan teknologi deepfake kini semakin meluas dan beragam bentuknya. Salah satu contoh video deepfake yang paling terkenal di internet adalah video Sri Mulyani yang mengatakan bahwa "Guru adalah beban Negara". Video tersebut menjadi peringatan bahwa penerapan deepfake sangat riskan dan membahayakan, sehingga pengguna perlu lebih waspada dalam mengakses konten internet selama ini.

Salah satu isu utama dari kejahatan deepfake yang paling menonjol dan mengkhawatirkan adalah deepfake pornografi, di mana wajah seseorang, tanpa persetujuan, ditempelkan (*face-swapped*) ke dalam video atau gambar yang bermuatan seksual. Berbagai laporan, termasuk dari penyedia layanan deteksi *Artificial Intelligence (AI)*, secara konsisten menunjukkan bahwa sekitar 96% dari konten *deepfake* yang beredar di internet adalah non-konsensual pornografi. Fenomena ini telah dikategorikan sebagai salah satu bentuk paling merusak dari Kekerasan Berbasis Gender Online KBGO (ARSLAN, 2023). Dalam kasus ini, penukaran wajah dapat digunakan untuk membuat deepfake siapa saja asalkan gambar wajah korban cukup. Menurut Ajder et al. (2019) Audio pidato yang akan diucapkan John F. Kennedy di Dallas pada 22 November 1963 adalah ilustrasi menarik lainnya. Perusahaan sintesis canggih Cere Proc membuat audio tersebut, yang disajikan pada bulan Maret 2018. Ini adalah pidato yang akan disampaikan Kennedy jika dia tidak terbunuh (Floridi 2021).

Penyebaran lebih lanjut dari deepfakes dapat mengganggu dinamika politik dalam negeri dan internasional. Diakopoulos dan Johnson (2021) menekankan beberapa cara teknologi deepfake ini mengganggu pemilihan umum. Hal ini terlihat dari video palsu yang menampilkan pernyataan dan komentar rasis serta saling menghina antar politisi yang bersaing. Selain itu, teknik deepfake ini dapat digunakan dengan cara yang lebih halus untuk memanipulasi hasil pemilu. Salah satu contohnya adalah "crowd-turfing", sebuah teknik yang digunakan dalam pemasaran dan kampanye untuk memberi kesan apakah dukungan rakyatnya atau tidak (De Ruiter, 2021).

Permasalahan selanjutnya muncul di dunia kestabilan pasar saham. Westerlund menyoroti bahwa teknologi *Artificial Intelligence (AI)* yang canggih telah digunakan untuk Kejahatan *deepfake* memungkinkan pelaku pasar untuk memanipulasi harga saham secara cepat dan masif melalui informasi palsu yang direayasa agar terlihat otentik. Fenomena *deepfake* yang telah diuraikan



sebelumnya, secara umum, merupakan manifestasi dari kompleksitas permasalahan yang bersifat komprehensif di tengah masyarakat. Secara fundamental, masalah ini berakar pada berbagai kepentingan, baik kepentingan individu, kelompok, maupun sosial budaya yang kemudian diperparah dan didorong oleh perkembangan teknologi yang berkembang pesat dan tidak terkendali. Kombinasi faktor kepentingan dan kemajuan teknologi inilah yang menjadi pemicu utama maraknya fenomena *deepfake* di ruang publik. (Ali et al., 2022)

Penjelasan tersebut menunjukkan bahwa meskipun tinjauan tentang penggunaan teknologi *deepfake* tidak menyeluruh, itu menunjukkan bahwa masalah yang muncul akan mengganggu atau menimbulkan masalah etika yang signifikan. Fenomena *deepfake* adalah ancaman dari segala arah yang muncul akibat permasalahan kepentingan sosial, individu, dan golongan yang diperparah oleh pesatnya perkembangan teknologi *Artificial Intelligence (AI)* yang tidak terkendali. Ancaman ini bermanifestasi secara luas, mulai dari dominasi konten pornografi non-konsensual (mencapai sekitar 96% dari total *deepfake* dan dikategorikan sebagai KBGO) yang merusak individu, penyebaran disinformasi politik dan manipulasi pemilu (*crowd-turfing*), hingga kejahatan manipulasi pasar saham melalui informasi palsu yang direayasa, sehingga menuntut pengguna internet untuk lebih berhati-hati dan bijak dalam merespons informasi digital guna mencegah kekacauan dan kerugian yang ditimbulkan.

4. KESIMPULAN

perkembangan teknologi *deepfake* telah menimbulkan tantangan baru dalam keamanan siber. teknologi ini memungkinkan individu dengan niat tertentu untuk menciptakan manipulasi video maupun audio yang sangat realistis sehingga sulit dibedakan dari konten asli. Beberapa kasus di Indonesia, seperti penyebaran video palsu yang melibatkan tokoh publik dan pejabat pemerintahan, membuktikan video palsu yang melibatkan tokoh publik dan pejabat pemerintahan, membuktikan bahwa *deepfake* dapat di jadikan sarana untuk menipu masyarakat, menyebarkan hoaks, serta menimbulkan kerugian finansial maupun psikologis bagi korban. Kemajuan teknologi informasi dan komunikasi memang telah memberikan kemudahan luar biasa bagi kehidupan manusia, namun kemudahan tersebut juga membawa tanggung jawab besar dalam penggunaannya. Dengan munculnya teknologi AI seperti *deepfake*, kemampuan literasi digital menjadi aspek yang sangat penting untuk dimiliki oleh setiap pengguna internet. Masyarakat harus dibekali kemampuan berpikir kritis, keterampilan memilah informasi, serta tanggung jawab etis dalam berinteraksi di dunia maya. Peningkatan literasi digital tidak hanya membantu pengguna dalam melindungi diri dari hoaks dan penipuan daring, tetapi juga mendorong terbentuknya peradaban digital yang cerdas, beretika, dan bermartabat.

REFERENCES

- Ali, A., Khan Ghouri, K. F., Naseem, H., Soomro, T. R., Mansoor, W., & Momani, A. M. (2022). Battle of Deep Fakes: Artificial Intelligence Set to Become a Major Threat to the Individual and National Security. 2022 *International Conference on Cyber Resilience (ICCR)*, 1–5. <https://doi.org/10.1109/ICCR56254.2022.9995821>
- ARSLAN, F. (2023). Deepfake Technology: A Criminological Literature Review. *Sakarya Üniversitesi Hukuk Fakültesi Dergisi*, 11(1), 701–720. <https://doi.org/10.56701/shd.1293642>
- De Ruiter, R. (2021). Political disinformation and the rise of deepfakes. *European Political Science Review*, 13(3), 412–427.
- Diakopoulos, N., & Johnson, D. (2021). Anticipating and addressing the ethical implications of deepfakes in the context of elections. *New Media & Society*, 23(7), 2072–2098. <https://doi.org/10.1177/1461444820925811>
- Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135–146. <https://doi.org/10.1016/j.bushor.2019.11.006>
- Mohamed, S., Png, M.-T., & Isaac, W. (2020). Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence. *Philosophy & Technology*, 33(4), 659–684. <https://doi.org/10.1007/s13347-020-00405-8>
- Mutmainnah, A., Suhandi, A. M., & Herlambang, Y. T. (2024). Problematika Teknologi Deepfake sebagai Masa Depan Hoax yang Semakin Meningkat: Solusi Strategis Ditinjau dari Literasi Digital. *UPGRADE: Jurnal Pendidikan Teknologi Informasi*, 1(2), 67–72. <https://doi.org/10.30812/upgrade.v1i2.3702>



JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 8, Januari Tahun 2026
ISSN 3025-0919 (media online)
Hal 2127-2131

- Nisa, K. (2024). The Role of Literacy in the Digital Era in Dealing with Hoaxes and Disinformation on Social Media. *Impressive: Journal of Education*, 2(1), 1–11.
- Saiyad Mahmmadakram Hanif, & Vivek Dave. (2022). Deepfakes Technology Using AI. *International Journal of Scientific Research in Science, Engineering and Technology*, 152–159. <https://doi.org/10.32628/IJSRSET229522>
- Shevila Kristiyenda, Y., Faradila, J., & Basanova, C. (n.d.). *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora Volume 3 Nomor 2 April 2025 Pencegahan Kejahatan Deepfake: Studi Kasus terhadap Modus Penipuan Deepfake Prabowo Subianto dalam Tawaran Bantuan Uang*.