BIN : Bulletin Of Informatics
Volume 3, No. 1 Juli 2025
ISSN 3025-7417 (media online)
Hal 68-72

Etika Profesi Informatika dalam Penyalahgunaan *AI Voice Cloning* dan *Deepfake*: Studi Kasus Penipuan Digital yang Diungkap OJK

Nita Sintia Nabila[1], Shalsa Tri Nagita[2], Adithea Vierninda[3], Kevin Sianpar[4], Annisa Elfina Augustia[5]

[1,2,3,4,5]Fakultas Teknik Informatika, Teknik Informatika, Universitas Indraprasta PGRI, Jakarta, Indonesia
Email: [2]shalsatrinagita@gmail.com, [5]annisa12elfina@gmail.com

Abstrak−Dalam dinamika perkembangan masyarakat modern, perkembangan teknologi kecerdasan buatan (AI) dapat membawa berbagai dampak bagi pengguna, salah satu dampak yang paling sering muncul ialah penyalahgunaan seperti *voice cloning* dan *deepfake* yang dapat merugikan banyak pihak. Penelitian ini dilakukan dengan alasan banyaknya kasus penipuan digital pada Otoritas Jasa Keuangan (OJK). Penelitian ini difokuskan untuk menganalisis pelanggaran etika profesi informatika dalam penggunaan teknologi AI yang disalahgunakan pada kasus penipuan digital yang diungkap oleh Otoritas Jasa Keuangan (OJK). Metode penelitian yang digunakan ialah kualitatif deskriptif dengan pendekatan studi literatur dari laporan resmi OJK, artikel, jurnal ilmiah, serta data dan berita yang diungkap OJK. Hasil analisis mengindikasikan bahwa penyalahgunaan v*oice cloning* dan *deepfake* menimbulkan pelanggaran terhadap prinsip etika profesional, khususnya tanggung jawab sosial, integritas, dan keamanan informasi. Temuan penelitian menegaskan perlunya tanggung jawab etis dari para profesional informatika, disertai dukungan regulasi yang lebih kuat dari pemerintah dalam mengawasi penerapan teknologi AI agar tidak disalahgunakan.

Kata Kunci: etika profesi Informatika; kecerdasan buatan (AI); *voice cloning; deepfake*; penipuan digital; Otoritas Jasa Keuangan (OJK)

Abstract−*In the dynamics of modern society, the development of artificial intelligence (AI) technology can bring various impacts to its users. One of the most common negative impacts is its misuse, such as voice cloning and deepfake, which can cause significant harm to many parties. This research was conducted due to the increasing number of digital fraud cases reported by the Financial Services Authority (OJK). The study focuses on analyzing violations of professional informatics ethics in the use of AI technology that has been misused in digital fraud cases revealed by OJK. The research employs a qualitative descriptive method with a literature study approach, utilizing official OJK reports, academic journals, scientific articles, and verified news data. The analysis results indicate that the misuse of voice cloning and deepfake leads to violations of professional ethical principles, particularly social responsibility, integrity, and information security. The findings emphasize the necessity for ethical responsibility among informatics professionals, accompanied by stronger regulatory support from the government to ensure that AI technology is used responsibly and not for harmful purposes.*

Keywords: *informatics professional ethics; Artificial Intelligence; voice cloning; deepfake;digital fraud;* Otoritas Jasa Keuangan (OJK)

1. PENDAHULUAN

Perkembangan teknologi yang cepat, terutama dalam buatan, telah memberikan pengaruh besar pada beragam kehidupan manusia. Saat ini, teknologi AI mampu melaksanakan berbagai tugas yang dulunya hanya bisa dilakukan oleh manusia, seperti mendukung proses kerja dan menciptakan karya kreatif dalam bentuk suara dan video yang menyerupai aslinya.

Salah satu inovasi yang menarik perhatian adalah teknologi peniruan suara dan *deepfake*. Kedua teknologi ini memiliki potensi luar biasa di sektor industri kreatif, pendidikan, dan hiburan. Meski demikian, di balik keuntungan yang ditawarkannya, terdapat pula sejumlah masalah etis dan sosial akibat penyalahgunaan teknologi ini. Contoh umum dari penyalahgunaan adalah penipuan digital, di mana pelaku memanfaatkan teknologi ini untuk meniru identitas orang lain demi memperoleh keuntungan pribadi.

Dengan demikian, meskipun kecerdasan buatan memberikan banyak kemudahan dan inovasi, penggunaannya harus diimbangi dengan pengawasan, regulasi, serta kesadaran etika agar dampak negatif seperti penyebaran informasi palsu dan kejahatan digital dapat diminimalkan. Di Indonesia, Otoritas Jasa Keuangan (OJK) pernah mengidentifikasi beberapa kasus penipuan digital yang menggunakan teknologi cloning suara dan deepfake. Dalam insiden tersebut, penipu memanfaatkan suara yang dipalsukan atau video yang menunjukkan individu seakan-akan merupakan pejabat

BIN : Bulletin Of Informatics
Volume 3, No. 1 Juli 2025
ISSN 3025-7417 (media online)
Hal 68-72

pemerintah. Tujuan dari tindakan tersebut adalah untuk mengecoh masyarakat agar mempercayai informasi yang mereka terima dan akhirnya melakukan transaksi keuangan atau menyuplai dana kepada pihak-pihak yang tidak dapat dipercaya. Kejadian ini menunjukkan bahwa penyalahgunaan teknologi kecerdasan buatan dapat memicu ancaman serius terhadap keamanan dunia maya dan kepercayaan masyarakat, sehingga diperlukan langkah-langkah pengawasan dan pendidikan untuk menjaga agar masyarakat tidak mudah terjebak oleh konten yang dimanipulasi berbasis AI.

Dari peristiwa ini, muncul pertanyaan krusial mengenai posisi etika dalam bidang informatika ketika teknologi dimanfaatkan untuk kepentingan yang merugikan atau menyimpang dari norma-norma moral. Dengan demikian, penelitian ini berusaha untuk mengeksplorasi aspek etika dan tanggung jawab profesional dalam dunia informatika, terutama yang berkaitan dengan penggunaan teknologi kecerdasan buatan (AI). Melalui analisis ini, diharapkan bisa diperoleh pemahaman yang lebih mendalam tentang batasan moral dan tanggung jawab profesional yang perlu dimiliki oleh pengembang serta pengguna teknologi, agar inovasi yang diciptakan tetap memberikan manfaat bagi masyarakat.

2. METODE PENELITIAN

Penelitian ini menerapkan metode kualitatif deskriptif dengan pendekatan satu studi kasus. Pemilihan metode ini didasarkan pada kemampuannya untuk menghasilkan wawasan mendalam tentang fenomena penyalahgunaan teknologi kecerdasan buatan (AI), khususnya dalam bentuk *cloning* suara dan deepfake yang dimanfaatkan sebagai alat penipuan digital di Indonesia. Penelitian ini berfokus pada beberapa kejadian yang diungkap oleh Otoritas Jasa Keuangan (OJK).

2.1 Satuan dan Lokasi Analisis

Dalam penelitian ini, unit yang dianalisis adalah skenario penipuan berbasis digital yang menggunakan teknologi *clon* suara dan *deepfake* yang telah teridentifikasi oleh OJK. Penelitian ini difokuskan pada sudut pandang etika profesi dibidang informatikaterutama mengenai pelanggaran terhadap nilai-nilai profesional serta tanggung jawab moral dalam penerapan teknologi AI di sektor digital di Indonesia.

2.2 Asal dan Kategori Data

Material yang digunakan dalam studi ini tergolong kualitatif dan diklasifikasikan menjadi dua kategori utama:

a. Data Primier (Dokumen resmi)
   Terdiri dari laporan resmi OJK, siaran pers, serta publikasi dari instansi pemerintah atau lembaga keamanan siber yang berkaitan dengan kasus penipuan digital yang berbasis AI.
b. Data Sekunder (Kajian Literatur)
   Meliputi artikel jurnal ilmiah, buku, prosiding, dan berita yang dapat dipercaya yang membahas fenomena peniruan suara, *deepfake*, serta analisis etika dan tanggung jawab profesional di bidang informatika.

2.3 Metode Pengumpulan dan Analisis Data

Cara pengumpulan data dilakukan dengan mengevaluasi literatur dan menganalisis dokumen yang relevan. Data yang diperoleh selanjutnya dianalisis menggunakan pendekatan deskriptif dan tematik untuk mengidentifikasi jenis-jenis pelanggaran etika serta norma profesional yang dilanggar dalam insiden penyalahgunaan teknologi AI. Proses evaluasi dilaksanakan melalui tiga tahap utama, yaitu:

1. Pengurangan data
   Memilih dan mengarahkan data pada informasi yang penting, seperti bentuk penyalahgunaan *voice cloning* dan *deepfake,* dampaknya bagi masyarakat, serta tanggapan OJK terhadap kejadian tersebut.
2. Penyajian data
   Menyampaikan hasil evaluasi dalam bentuk narasi deskriptif yang menjelaskan pola penyalahgunaan teknologi, konteks etika profesi, serta norma moral yang dilanggar.
3. Penarikan kesimpulan

BIN : Bulletin Of Informatics
Volume 3, No. 1 Juli 2025
ISSN 3025-7417 (media online)
Hal 68-72

Menerjemahkan hasil evaluasi berdasarkan teori Etika Profesi Informatika dan prinsip Tanggung Jawab Profesional dengan tujuan merumuskan pandangan etis serta rekomendasi terkait penggunaan AI agar sejalan dengan nilai moral dan profesionalisme di bidang informatika.

3. ANALISIS DAN PEMBAHASAN

Dari pemeriksaan terhadap laporan resmi Otoritas Jasa Keuangan (OJK, 2024) dan beberapa artikel berita yang dapat dipercaya, teridentifikasi beberapa pola penyalahgunaan teknologi *voice cloning* dan *deepfake* dalam kasus penipuan digital di Indonesia. Pelaku memanfaatkan rekayasa suara dan video untuk meniru identitas pejabat di lembaga keuangan atau tokoh publik dengan tujuan meyakinkan korban agar melakukan transfer dana atau memberikan informasi pribadi.

Teknologi *voice cloning* memanfaatkan model *text-to-speech* berbasis *machine learning* yang mampu meniru intonasi, tempo, dan karakteristik suara seseorang hanya dengan menggunakan sampel audio singkat (Susanto & Wirawan, 2023). Sebaliknya, *deepfake* menggunakan jaringan neural mendalam untuk mengubah wajah atau ekspresi seseorang dalam video agar terlihat seolah-olah nyata (Rahmadani, 2022). Sebenarnya, kedua teknologi ini dirancang untuk tujuan yang positif, seperti produksi film, pendidikan, atau pengembangan asisten digital. Namun, dalam praktiknya, pelaku kejahatan siber justru memanfaatkan keduanya sebagai alat manipulasi sosial yang sulit dikenali oleh masyarakat umum. Situasi ini menunjukkan adanya kesenjangan antara kemajuan teknologi dan kesadaran etis dalam penggunaannya (Putra, 2024).

3.1 Tinjauan Etika dalam Bidang Informatika Terkait Penyalahgunaan Kecerdasan Buatan (AI)

Dari sudut pandang etika dalam profesi informatika, penyalahgunaan teknologi *cloning suara* dan *deepfake* termasuk ke dalam kategori pelanggaran terhadap prinsip integritas, tanggung jawab, serta kejujuran dalam profesi. Berdasarkan Kode Etik Profesional Informatika (ACM, 2020), seorang ahli di sektor teknologi informasi diwajibkan untuk tidak memanfaatkan keahlian teknisnya dengan cara yang dapat merugikan individu atau masyarakat luas. Dalam situasi ini, pelaku dengan sengaja memanfaatkan kecerdasan buatan untuk meniru identitas dan menipu targetnya. Perbuatan ini melanggar nilai utama *non-maleficence*, yaitu kewajiban untuk tidak menyebabkan kerugian melalui penggunaan teknologi yang telah diciptakan (Floridi, 2019). Di samping itu, dari perspektif tanggung jawab sosial, para pengembang dan penyedia layanan kecerdasan buatan memiliki kewajiban moral untuk memastikan bahwa sistem yang mereka buat tidak rentan terhadap penyalahgunaan. Hal ini mencakup penerapan langkah keamanan, autentikasi suara atau video, serta *digital watermarking* yang dapat membantu mendeteksi konten tidak asli. Dengan demikian, etika dalam profesi informatika tidak hanya menjadi tanggung jawab pelaku pelanggaran, tetapi juga mencakup pihak yang berperan dalam pengembangan dan penyediaan teknologi kecerdasan buatan (Widodo, 2023).

3.2 Konsekuensi dan Tantangan Etis untuk Professional Teknologi Informasi

Penyalahgunaan kecerdasan buatan dalam *cloning suara* dan *deepfake* menimbulkan dampak yang beragam. Dari sisi sosial, masyarakat menjadi lebih rentan terhadap penipuan digital yang bergantung pada kepercayaan visual dan auditori serta memanfaatkan psikologi korban sehingga mendorong pengambilan keputusan tanpa verifikasi kebenaran. Dari aspek ekonomi, kerugian muncul akibat transaksi yang tidak sah. Dari perspektif etika, tingkat kepercayaan terhadap teknologi juga mengalami penurunan yang signifikan (OJK, 2024).

Bagi para profesional di bidang teknologi informasi, tantangan etis yang utama adalah menemukan keseimbangan antara inovasi dan tanggung jawab terhadap masyarakat. Baik mahasiswa maupun praktisi di bidang ini perlu menyadari bahwa perkembangan kecerdasan buatan berkaitan erat dengan pertimbangan moral dan hukum. Penggunaan teknologi tanpa memperhatikan etika dapat menimbulkan risiko besar terhadap privasi, keamanan data, serta integritas profesi teknologi informasi itu sendiri (Nugroho, 2024).Oleh karena itu, penguatan pendidikan etika profesi di ranah akademis dan organisasi profesional menjadi hal yang penting agar setiap pihak yang terlibat dalam pengembangan teknologi memahami batasan moral penggunaan kecerdasan buatan. Pendekatan *ethical by design*, yaitu integrasi prinsip etika sejak tahap awal perancangan teknologi,

BIN : Bulletin Of Informatics
Volume 3, No. 1 Juli 2025
ISSN 3025-7417 (media online)
Hal 68-72

menjadi solusi krusial untuk mencegah penyalahgunaan di masa mendatang (Floridi & Cowls, 2021).

3.3 Dampak pada Etika dan Peraturan di Indonesia

Situasi yang diungkapkan oleh Otoritas Jasa Keuangan menunjukkan bahwa peraturan yang mengatur penggunaan kecerdasan buatan di Indonesia belum sepenuhnya siap untuk menghadapi tantangan etis dan hukum dari teknologi seperti *deepfake* dan *cloning suara*. Meskipun Undang-Undang Informasi dan Transaksi Elektronik telah diberlakukan, penerapannya masih terbatas pada penyebaran informasi palsu dan pencemaran nama baik, tanpa pengaturan khusus terkait penyalahgunaan AI dalam penipuan digital (Kementerian Kominfo, 2024).

Dari perspektif profesi informatika, terdapat kebutuhan untuk menerapkan kode etik yang lebih responsif terhadap perkembangan AI, termasuk penegasan tanggung jawab etis bagi pengembang sistem untuk melakukan pengujian keamanan dan strategi mitigasi risiko penyalahgunaan. Upaya seperti sertifikasi etika profesional, pelatihan tanggung jawab sosial, serta audit etika teknologi perlu dipertimbangkan guna menjaga kepercayaan masyarakat terhadap bidang informatika di Indonesia (Putra & Hartono, 2024).

4. KESIMPULAN

Mengacu pada hasil kajian yang telah dilakukan, dapat disimpulkan bahwa penyalahgunaan teknologi kecerdasan buatan dalam bentuk *cloning suara* dan *deepfake* bukan hanya merupakan masalah teknis, tetapi juga berkaitan dengan pelanggaran prinsip etika dalam profesi informatika, khususnya nilai integritas, tanggung jawab, dan kejujuran professional. Studi ini menunjukkan bahwa insiden penipuan digital yang diidentifikasi oleh Otoritas Jasa Keuangan mencerminkan rendahnya kesadaran etis dalam penerapan teknologi kecerdasan buatan. Keahlian teknis yang seharusnya dimanfaatkan untuk mendukung kemajuan masyarakat justru disalahgunakan untuk merugikan pihak lain. Kondisi ini menandakan adanya ketidakseimbangan antara pesatnya perkembangan teknologi dan kesadaran moral, baik dari sisi pengguna maupun pengembang.

Dari perspektif etika profesi informatika, manipulasi identitas melalui *cloning suara* dan *deepfake* jelas melanggar prinsip *non-maleficence*, yaitu kewajiban untuk tidak menimbulkan kerugian, serta melanggar tanggung jawab sosial profesi. Prinsip tersebut menegaskan bahwa setiap profesional informatika bertanggung jawab atas dampak sosial dari teknologi yang mereka kembangkan atau gunakan. Dalam konteks ini, pelaku kejahatan siber secara sadar memanfaatkan kecerdasan buatan untuk menipu masyarakat, yang pada akhirnya menurunkan kepercayaan publik terhadap teknologi dan lembaga resmi.

Penelitian ini juga menekankan pentingnya sinergi antara regulasi, kesadaran etis, dan pendidikan moral dalam menghadapi ancaman penyalahgunaan kecerdasan buatan. Pemerintah melalui lembaga terkait perlu memperkuat regulasi yang lebih spesifik terhadap praktik *cloning* suara dan *deepfake*. Di sisi lain, institusi pendidikan serta organisasi profesi informatika perlu menanamkan nilai etika dan tanggung jawab sosial secara sistematis kepada calon profesional sejak dini.

Oleh karena itu, kemajuan teknologi kecerdasan buatan harus selalu disertai dengan kesadaran etis dan moral dalam praktik profesi. Penerapan prinsip *ethical by design* menjadi langkah strategis agar teknologi yang dikembangkan tidak hanya unggul secara teknis, tetapi juga mengutamakan keselamatan dan kepentingan publik. Kolaborasi antara akademisi, praktisi, dan pemerintah menjadi faktor kunci untuk memastikan pengembangan kecerdasan buatan berlangsung secara bertanggung jawab serta memberikan manfaat nyata bagi masyarakat tanpa mengancam nilai-nilai kemanusiaan.

REFERENCES

Association for Computing Machinery (ACM). (2018). ACM Code of Ethics and Professional Conduct. New York: ACM. Tersedia di: https://www acm.org/code-of-ethics

Chesney, B., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107(6), 1753-1820.

BIN : Bulletin Of Informatics
Volume 3, No. 1 Juli 2025
ISSN 3025-7417 (media online)
Hal 68-72

Floridi, L., et al. (2018). AI4People: An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines, 28(4), 689-707.

Kompas.com. (2024). Video Deepfake Jusuf Hamka Beredar, OJK Ingatkan Bahaya Penipuan Investasi Bodong. Diakses dari: [Masukkan URL Berita Aktual].

Otoritas Jasa Keuangan. (2024). Waspada Kejahatan Digital: Modus Penipuan Mengatasnamakan OJK dan Pelaku Jasa Keuangan. Sikapi Uangmu OJK. Tersedia di: https://sikapiuangmu.ojk.go.id

Pemerintah Republik Indonesia. (2024). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2024 Nomor 10. Jakarta: Sekretariat Negara.

Situmeang, A. (2021). Penyalahgunaan Data Pribadi Melalui Teknologi Deepfake di Indonesia: Perspektif Hukum dan Etika. Jurnal Hukum & Pembangunan, 51(3), 738-752.