Jurnal Ilmiah Multidisiplin
https://ejournal.lumbungpare.org/index.php/jim
DOI: https://doi.org/10.60126/jim.v4i4.1563
e-ISSN 3026-3808

Tinjauan Etika Profesi Teknologi Informasi Terhadap *Deepfake Harassment* di Media Sosial: *Systematic Literature Review*

Evy Nurmiati[1], Fathiyah Nur Rizqi[1*]

[1]Program Studi Sistem Informasi, UIN Syarif Hidayatullah Jakarta, Indonesia
*Corresponding author : fathiyah.nur24@mhs.uinjkt.ac.id

Article History:
Received : 25-04-2026
Accepted : 30-04-2026

Keywords: Deepfake; Harassment; Etika Profesi TI; Kecerdasan Buatan; Media Sosial; Perlindungan Hukum

ABSTRAK

Kemajuan kecerdasan buatan (AI), khususnya teknologi *deepfake*, telah melahirkan pola baru pelecehan seksual berbasis digital yang mengancam integritas individu di ruang siber. Fenomena ini menghadirkan tantangan serius bagi etika profesi Teknologi Informasi (TI) yang selama ini menjadi landasan moral bagi para pelaku industri digital. Artikel ini bertujuan menganalisis secara kritis fenomena *deepfake harassment* di media sosial dalam kerangka kode etik profesi TI, mengidentifikasi celah regulasi hukum di Indonesia, serta merumuskan rekomendasi praktis bagi profesional TI. Penelitian menggunakan pendekatan *Systematic Literature Review* (SLR) dengan protokol PRISMA. Pencarian dilakukan melalui Google Scholar menggunakan kata kunci "*deepfake*", "*harassment*", "etika teknologi informasi", dan "*AI ethics*". Dari 87 artikel teridentifikasi, sebanyak 6 artikel memenuhi kriteria inklusi untuk dianalisis secara mendalam. Literatur menunjukkan bahwa *deepfake harassment* melanggar setidaknya lima prinsip utama dalam ACM Code of Ethics dan IEEE Code of Ethics, yaitu prinsip kejujuran, *non-maleficence*, privasi, akuntabilitas, dan tanggung jawab sosial. Regulasi hukum Indonesia (UU ITE, UU TPKS, UU PDP) belum secara spesifik mengakomodasi penyalahgunaan *AI*, sehingga menimbulkan celah normatif dalam penegakan hukum. Diperlukan pembaruan kode etik profesi TI yang responsif terhadap ancaman *deepfake*, penguatan regulasi berbasis *AI*, serta peningkatan literasi digital masyarakat secara sistematis.

PENDAHULUAN

Perkembangan teknologi digital, khususnya kecerdasan buatan (*AI*), telah menghadirkan inovasi yang mengubah cara manusia berproduksi dan berkomunikasi secara mendasar. Salah satu manifestasi paling mengkhawatirkan dari kemajuan ini adalah teknologi *deepfake*, yaitu teknik manipulasi konten audio, video, gambar, dan teks menggunakan algoritma *deep learning* sehingga menghasilkan konten palsu yang sangat realistis dan sulit dibedakan dari konten asli [1]. Teknologi ini, meskipun awalnya dikembangkan untuk keperluan hiburan dan riset, dengan cepat disalahgunakan untuk berbagai tindakan merugikan, termasuk pelecehan seksual berbasis digital.

Deepfake harassment merujuk pada penggunaan teknologi *deepfake* untuk menciptakan konten bermuatan seksual atau merendahkan martabat seseorang tanpa persetujuannya, kemudian menyebarkannya melalui platform media sosial. Fenomena ini telah melahirkan bentuk baru *sexual harassment* di ruang siber yang berdampak signifikan terhadap kondisi psikologis, relasi sosial, dan kehormatan diri korban [2]. Lebih jauh, Fitri et al. (2025) mencatat bahwa penelitian menunjukkan 47% dari kasus penyalahgunaan *deepfake* yang

dianalisis berkaitan dengan pelecehan personal, sementara sekitar 32% berkaitan dengan disinformasi politik.

Di tengah maraknya fenomena ini, perhatian terhadap aspek etika profesi Teknologi Informasi (TI) masih sangat terbatas dalam literatur akademik Indonesia. Para profesional TI, mulai dari pengembang algoritma, perancang platform media sosial, hingga administrator sistem, memiliki tanggung jawab moral yang besar dalam mencegah atau setidaknya memitigasi dampak teknologi yang mereka kembangkan dan kelola. Kode etik profesi internasional seperti ACM Code of Ethics (2018) dan IEEE Code of Ethics menetapkan sejumlah prinsip fundamental, antara lain kejujuran, *non-maleficence*, dan penghormatan terhadap privasi, yang seharusnya menjadi panduan dalam pengembangan dan pengelolaan teknologi *AI*.

Namun, terdapat kesenjangan yang signifikan antara norma etika profesi yang ada dengan realitas penyalahgunaan teknologi *deepfake*. Leliana et al. (2023) mengidentifikasi bahwa untuk menjaga integritas komunikasi dalam era *deepfake* diperlukan upaya kolaboratif dari masyarakat, pemerintah, lembaga, dan individu, termasuk para profesional TI [3]. Di sisi hukum, Erdiyanti et al. (2026) menemukan bahwa meskipun Indonesia telah memiliki sejumlah instrumen hukum seperti UU ITE, UU TPKS, dan UU PDP, pengaturan mengenai penyalahgunaan teknologi *AI* masih bersifat parsial dan belum secara khusus mengatur *deepfake* pornografi, sehingga menimbulkan celah dalam penegakan hukum.

Artikel ini hadir untuk mengisi kesenjangan tersebut dengan menawarkan analisis sistematis yang mempertemukan perspektif etika profesi TI dengan fenomena *deepfake harassment*. Kebaruan (novelty) penelitian ini terletak pada pendekatan integratif yang menghubungkan kode etik profesi TI internasional dengan konteks hukum dan sosial Indonesia, sesuatu yang belum banyak dilakukan oleh studi sebelumnya. Kontribusi ilmiahnya adalah tersedianya peta pelanggaran etika yang terstruktur serta rekomendasi operasional bagi profesional TI dalam menghadapi tantangan *deepfake*.

Tujuan penelitian ini adalah untuk mengidentifikasi bentuk-bentuk pelanggaran etika profesi Teknologi Informasi (TI) yang terkandung dalam fenomena *deepfake harassment*, menganalisis kecukupan regulasi hukum di Indonesia dalam merespons kejahatan berbasis *deepfake*, serta merumuskan rekomendasi praktis bagi para profesional TI. Sejalan dengan tujuan tersebut, penelitian ini juga berupaya menjawab pertanyaan utama mengenai bagaimana fenomena *deepfake harassment* di media sosial dapat dianalisis melalui perspektif etika profesi TI, serta apa implikasinya terhadap pembaruan regulasi dan praktik profesional di bidang teknologi informasi.

METODE PENELITIAN

Penelitian ini menggunakan metode *Systematic Literature Review* (SLR) yang mengikuti protokol PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*). Metode PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) merupakan pedoman standar berbasis bukti yang terdiri dari checklist 27 item dan diagram alur, yang digunakan untuk melaporkan tinjauan sistematis dan meta-analisis secara transparan, sistematis, dan terstruktur. Metode ini bertujuan untuk menjamin kualitas yang tinggi dalam proses seleksi studi. SLR dipilih karena kemampuannya dalam mensintesis

temuan dari berbagai studi secara transparan, terstruktur, dan dapat direplikasi, sehingga menghasilkan gambaran komprehensif tentang keadaan pengetahuan pada topik yang dikaji.

Pencarian literatur dilaksanakan secara sistematis melalui mesin pencari akademik Google Scholar pada periode Maret hingga April 2025. Kata kunci yang digunakan meliputi, "*deepfake*", "*harassment*", "etika teknologi informasi", "*AI ethics*", "*deepfake harassment*", "pelecehan digital *AI*", dan kombinasinya menggunakan operator Boolean AND dan OR. Pencarian dibatasi pada artikel berbahasa Indonesia dan Inggris yang diterbitkan antara tahun 2019 hingga 2025.

Tabel 1. Kriteria Inklusi dan Eksklusi

Inklusi	Eksklusi
Artikel jurnal ilmiah yang diterbitkan pada jurnal nasional terakreditasi SINTA 1 sampai 4 atau jurnal internasional bereputasi.	Artikel opini atau editorial tanpa metodologi yang jelas.
Membahas teknologi *deepfake* dan/atau kecerdasan buatan dalam konteks pelecehan, disinformasi, atau etika.	Literatur abu-abu seperti laporan pemerintah yang tidak melalui proses peer review.
Diterbitkan pada rentang tahun 2019 hingga 2025.	Duplikasi Artikel.
Tersedia dalam teks lengkap dan relevan dengan konteks Indonesia atau memiliki implikasi yang dapat diterapkan pada konteks tersebut.	Artikel yang tidak membahas dimensi etika, hukum, atau sosial dari *deepfake*.

Tabel 1 menunjukkan bagaimana kriteria inklusi berfokus pada publikasi yang mutakhir dan relevan, sementara kriteria eksklusi bertujuan menghindari sumber non-akademik guna menjaga kualitas data. Proses seleksi artikel mengikuti empat tahapan PRISMA sebagaimana ditunjukkan dalam tabel 2 berikut ini.

Tabel 2. Alur Seleksi Artikel Berbasis PRISMA

Fase PRISMA	Keterangan	Jumlah Artikel	Keputusan
Identifikasi	Pencarian Google Scholar	87	Semua artikel
Screening	Seleksi judul & abstrak	34	Duplikat & tidak relevan dibuang
Eligibility	Baca teks lengkap	12	Di luar topik dieksklusi
Inclusion	Memenuhi kriteria inklusi	6	Dianalisis penuh

Pada tahap Identifikasi, ditemukan total 87 artikel melalui Google Scholar dengan menggunakan kata kunci yang telah ditetapkan. Tahap *Screening* mereduksi jumlah menjadi 34 artikel setelah penghapusan duplikat dan artikel yang tidak relevan berdasarkan judul dan abstrak. Pada tahap *Eligibility*, pembacaan teks lengkap menghasilkan 12 artikel yang secara substansi membahas dimensi etika atau hukum dari *deepfake*. Akhirnya, pada tahap *Inclusion*, sebanyak 6 artikel ditetapkan memenuhi seluruh kriteria inklusi dan menjadi korpus utama analisis dalam penelitian ini.

Analisis dilakukan melalui pendekatan tematik-kritis. Setiap artikel dianalisis untuk mengidentifikasi definisi dan karakteristik *deepfake* yang dibahas, dampak sosial dan

psikologis yang diidentifikasi, dimensi hukum yang disoroti, dan implikasi etika yang disebutkan atau tersirat. Temuan dari masing-masing artikel kemudian disintesis secara tematik dan dikontrastasikan dengan prinsip-prinsip dalam ACM Code of Ethics (2018) dan IEEE Code of Ethics untuk mengidentifikasi pola pelanggaran etika profesi TI.

HASIL DAN PEMBAHASAN

Karakteristik dan Tipologi *Deepfake* Harassment

Sintesis dari literatur yang dianalisis menunjukkan bahwa *deepfake harassment* bukan merupakan fenomena tunggal, melainkan sebuah spektrum tindakan berbahaya yang memanfaatkan teknologi manipulasi konten *AI*. Fitri et al. (2025) mengklasifikasikan konten *deepfake* ke dalam lima kategori utama yaitu, *deepfake* video, *deepfake* audio, *deepfake* gambar, *deepfake* teks, dan konten multimodal. Dalam konteks *harassment*, *deepfake* gambar dan video yang bermuatan seksual menjadi yang paling dominan dan paling merusak bagi korban. Proses pembuatannya yang semakin mudah diakses merupakan faktor peningkat risiko yang signifikan karena tidak memerlukan keahlian teknis khusus, mengingat banyaknya tutorial gratis yang tersedia di internet [4].

Zahro et al. (2024) memperkuat perspektif ini dengan menemukan bahwa konten *deepfake* yang beredar di media sosial umumnya bernuansa komedi dan hiburan, tetapi tidak jarang mengandung unsur negatif seperti pornografi dan berita bohong. Yang lebih mengkhawatirkan, riset mereka menemukan bahwa individu dengan pengetahuan rendah tentang teknologi *deepfake* cenderung mudah percaya pada konten manipulatif tersebut, menciptakan lingkaran setan yang memperparah dampak pelecehan. Sementara itu, Erdiyanti et al. (2026) menegaskan bahwa karakteristik konten *deepfake* yang sulit dibedakan dari konten asli menyebabkan kerugian yang dialami korban menjadi lebih berat dibandingkan bentuk kejahatan siber konvensional. Dalam konteks keamanan siber yang lebih luas, Huwaida et al. (2025) melalui kajian sistematis berbasis protokol PRISMA menemukan bahwa penyalahgunaan *deepfake* di ranah media sosial dan keamanan siber terus meningkat secara signifikan, dan mengidentifikasi munculnya fenomena *epistemic uncertainty*, yaitu kondisi di mana masyarakat kehilangan kepercayaan terhadap keaslian bukti visual akibat semakin canggihnya teknologi pemalsuan konten [5].

Dampak Sosial dan Psikologis

Dari aspek dampak, literatur secara konsisten mengidentifikasi tiga dimensi kerugian utama yang dialami korban *deepfake harassment*. Pertama, dimensi psikologis yang mencakup tekanan mental mendalam, trauma, rasa malu, dan gangguan kesehatan mental jangka panjang. Erdiyanti et al. (2026) menekankan bahwa rekayasa wajah, suara, atau identitas seseorang ke dalam konten bermuatan seksual tanpa persetujuan tidak hanya melanggar hak atas privasi dan martabat manusia, tetapi juga menimbulkan tekanan psikologis yang mendalam. Kondisi ini diperburuk oleh risiko reviktimisasi selama proses hukum berlangsung.

Kedua, dimensi sosial yang meliputi kerusakan reputasi, isolasi sosial, dan terganggunya hubungan interpersonal korban. Leliana et al. (2023) mencatat bahwa *deepfake* dapat digunakan untuk memanipulasi citra atau suara seseorang tanpa izin mereka, yang dapat menyebabkan potensi penyalahgunaan yang serius terhadap privasi individu. Ketiga, dimensi ekonomi yang mencakup kerugian finansial akibat penipuan berbasis *deepfake* audio yang

meniru suara eksekutif, di mana Fitri et al. (2025) melaporkan sekitar 21% dari penyalahgunaan *deepfake* berkaitan dengan penipuan semacam ini.

Pada level makro, dampak *deepfake harassment* juga mengancam fondasi kepercayaan publik terhadap informasi digital. Zahro et al. (2024) memperkenalkan konsep "*infopocalypse*" untuk menggambarkan situasi di mana masyarakat terperangkap dalam banjir hoaks yang sulit dibedakan dari fakta, mengakibatkan kebingungan dan ketidakpercayaan yang meluas. Kondisi ini, bila dibiarkan, dapat mengikis kemampuan masyarakat untuk membuat keputusan yang didasarkan pada fakta dalam kehidupan demokratis.

Pelanggaran Etika Profesi TI

Mengacu pada ACM Code of Ethics (2018) dan IEEE Code of Ethics, analisis tematik terhadap literatur yang diulas mengidentifikasi setidaknya lima kategori pelanggaran etika profesi TI yang terkandung dalam fenomena *deepfake harassment*.

Pertama, pelanggaran prinsip "*Avoid Harm*" (ACM 1.2 / IEEE). *Deepfake harassment* secara inheren bertujuan atau berujung pada pemberian kerugian nyata kepada individu. Profesional TI yang mengembangkan, menyebarkan, atau bahkan hanya memfasilitasi teknologi *deepfake* tanpa mengimplementasikan mekanisme mitigasi yang memadai telah melanggar prinsip ini. Fitri et al. (2025) menegaskan bahwa kemudahan pembuatan *deepfake* meningkatkan risiko penyebaran informasi palsu, manipulasi opini publik, dan kerusakan reputasi individu, yang kesemuanya merupakan bentuk kerugian yang dapat diantisipasi oleh profesional TI yang kompeten.

Kedua, pelanggaran prinsip "*Be Honest and Trustworthy*" (ACM 1.3). Inti dari *deepfake* adalah kepalsuan yang disengaja, yang secara fundamental bertentangan dengan kejujuran sebagai nilai inti profesi TI. Leliana et al. (2023) menyatakan bahwa masyarakat dan individu harus memiliki kewajiban moral untuk berkomunikasi dengan jujur, dan dalam konteks *deepfake*, penting untuk mempertahankan kejujuran komunikasi dan menghindari penyebaran konten palsu. Profesional TI yang merancang sistem yang memudahkan pembuatan konten palsu tanpa kontrol yang memadai berkontribusi pada erosi kepercayaan ini.

Ketiga, pelanggaran prinsip "*Respect Privacy*" (ACM 1.6 / IEEE). *Deepfake harassment* hampir selalu melibatkan penggunaan data biometrik seseorang, khususnya citra wajah dan suara, tanpa persetujuan. Erdiyanti et al. (2026) secara tegas menyatakan bahwa penggunaan data wajah dan identitas korban tanpa izin bertentangan dengan ketentuan UU PDP yang melarang pembuatan serta pemalsuan informasi pribadi. Dari perspektif etika profesi, pengembang sistem yang mengabaikan *privacy by design* dalam arsitektur platform mereka turut bertanggung jawab atas pelanggaran privasi massal yang terjadi.

Keempat, pelanggaran prinsip "*Accept and Provide Appropriate Professional Review*" dan "*Give Comprehensive and Thorough Evaluations*" (ACM 2.4 / 2.5). Profesional TI memiliki tanggung jawab untuk melakukan evaluasi menyeluruh terhadap dampak potensial dari teknologi yang mereka kembangkan sebelum merilisnya ke publik. Kegagalan industri teknologi dalam mengantisipasi dan mencegah penyalahgunaan deepfake secara luas mencerminkan absennya evaluasi etika yang memadai dalam siklus pengembangan produk.

Kelima, pelanggaran prinsip "*Contribute to Society and to Human Well-being*" (ACM 1.1). Prinsip tertinggi dalam kode etik ACM menuntut profesional TI untuk memprioritaskan kesejahteraan masyarakat. Rambe & Khoiri (2024) menemukan bahwa *cyberbullying* dalam berbagai bentuknya, termasuk *deepfake harassment*, mengambil bentuk argumen, fitnah, *body*

shaming, dan pelecehan yang secara langsung bertentangan dengan kesejahteraan sosial yang seharusnya diperjuangkan oleh profesional TI [6].

Regulasi Hukum Indonesia

Dari perspektif regulasi, terdapat temuan konvergen yang signifikan di seluruh literatur yang dianalisis, yaitu Indonesia belum memiliki kerangka hukum yang secara komprehensif dan spesifik mengatur penyalahgunaan teknologi *AI* dalam bentuk *deepfake*. Erdiyanti et al. (2026) mengidentifikasi bahwa meskipun perbuatan manipulasi konten digital berbasis *AI* dapat dijerat dengan UU Pornografi (No. 44/2008), UU ITE (No. 11/2008 jo. No. 1/2024), UU TPKS (No. 12/2022), dan UU PDP (No. 27/2022), pengaturan tersebut masih tergolong parsial serta tidak memiliki kejelasan normatif terkait penyalahgunaan teknologi *AI* secara spesifik. Seveney et al. (2025) dalam kajiannya terhadap UU No. 44 Tahun 2008 tentang Pornografi menegaskan bahwa undang-undang tersebut, yang dirancang sebelum era *AI* berkembang pesat, tidak secara tegas mencakup konten hasil manipulasi teknologi seperti *deepfake* sehingga menimbulkan celah hukum yang nyata [7]. Senada dengan itu, Quratuainniza dan Nurkhaerani (2025) menemukan bahwa UU ITE pun belum memberikan definisi yang eksplisit mengenai kecerdasan buatan maupun *deepfake*, sehingga menyulitkan aparat penegak hukum dalam menerapkan pasal-pasal yang relevan terhadap kasus-kasus terkait [8]. Dari sisi pertanggungjawaban pidana, Risno et al. (2025) menjelaskan bahwa pelaku *deepfake* pornografi pada dasarnya dapat dijerat melalui kombinasi tiga instrumen hukum sekaligus, yaitu UU ITE, UU Pornografi, dan UU PDP, di mana ketiga instrumen tersebut mengatur aspek yang berbeda namun saling melengkapi dalam memberikan sanksi berupa pidana penjara dan/atau denda [9].

Kondisi ini menimbulkan setidaknya tiga masalah praktis dalam penegakan hukum. Pertama, kesulitan pembuktian karena perkara pelecehan seksual nonfisik dan berbasis elektronik sangat bergantung pada alat bukti elektronik yang memerlukan keahlian forensik digital khusus. Kedua, tumpang tindih norma yang menyebabkan aparat penegak hukum kerap bingung memilih pengaturan yang paling tepat untuk diterapkan. Ketiga, risiko reviktimisasi selama proses hukum berlangsung, di mana korban terpaksa menjalani penyelidikan berulang yang memperburuk trauma psikologis (Erdiyanti et al., 2026).

Sebagai perbandingan, Uni Eropa melalui *Artificial Intelligence Act* telah lebih progresif dalam menyusun kerangka hukum yang adaptif terhadap teknologi baru. Indonesia perlu mengambil pelajaran dari pendekatan komprehensif tersebut. Fitri et al. (2025) merekomendasikan pendekatan sistemik yang melibatkan pembentukan regulasi hukum yang spesifik, peningkatan literasi digital masyarakat, dan pengembangan teknologi pendeteksi *deepfake* yang lebih akurat sebagai solusi terpadu.

Rekomendasi Untuk Profesional TI

Berdasarkan sintesis literatur dan analisis kritis yang telah dilakukan, artikel ini merumuskan tiga klaster rekomendasi bagi profesional TI dalam menghadapi tantangan *deepfake* harassment.

Klaster pertama adalah rekomendasi teknis. Pengembang platform dan algoritma TI perlu mengimplementasikan mekanisme deteksi *deepfake* secara proaktif dalam sistem mereka sebelum produk diluncurkan ke publik. Leliana et al. (2023) merekomendasikan penggunaan watermark atau tanda tangan digital pada materi asli untuk mencegah pemalsuan, serta pengembangan protokol untuk memverifikasi video atau audio yang mencurigakan. Selain itu,

penerapan prinsip *privacy by design* dalam setiap tahap pengembangan sistem merupakan kewajiban etis yang tidak dapat diabaikan.

Klaster kedua adalah rekomendasi kelembagaan. Organisasi profesi TI di Indonesia perlu melakukan pembaruan kode etik yang secara eksplisit mengakomodasi ancaman teknologi *AI*, termasuk deepfake. Zahro et al. (2024) menekankan bahwa menghadapi ancaman *deepfake* memerlukan upaya pendidikan dan kesadaran berkelanjutan. Perusahaan teknologi memiliki kewajiban etis untuk melatih karyawan mereka tentang potensi penyalahgunaan produk yang mereka kembangkan, serta membuat mekanisme pelaporan yang aman bagi pengguna yang menjadi korban.

Klaster ketiga adalah rekomendasi kebijakan. Profesional TI perlu terlibat aktif dalam proses perumusan regulasi nasional terkait *AI* dan *deepfake*, mengingat keahlian teknis mereka tidak tergantikan dalam merancang kebijakan yang efektif dan dapat diimplementasikan. Erdiyanti et al. (2026) menegaskan perlunya pembaruan regulasi yang lebih selaras dengan kemajuan teknologi dan menerapkan sistem perlindungan hukum yang berfokus pada korban. Quratuainniza dan Nurkhaerani (2025) mengusulkan penyusunan regulasi yang menyeluruh untuk mempertegas tanggung jawab para pengembang *AI*, meningkatkan pengawasan terhadap platform digital, serta memastikan adanya perlindungan bagi korban penyalahgunaan. Upaya ini perlu didukung melalui kerja sama antara pemerintah, kalangan akademisi, dan sektor swasta. Priana et al. (2025) menambahkan bahwa kolaborasi lintas sektor antara lembaga pemerintah, komunitas kreatif, dan organisasi masyarakat sipil dapat memperluas jangkauan dan memperkaya konten kebijakan yang dihasilkan.

KESIMPULAN

Penelitian ini menganalisis secara sistematis fenomena *deepfake harassment* di media sosial melalui perspektif etika profesi Teknologi Informasi berdasarkan sintesis enam artikel yang memenuhi kriteria SLR. Terdapat tiga temuan utama. Pertama, *deepfake harassment* merupakan pelanggaran multidimensi terhadap kode etik profesi TI, khususnya lima prinsip utama: menghindari kerugian, kejujuran, penghormatan privasi, evaluasi profesional yang komprehensif, dan kontribusi terhadap kesejahteraan masyarakat. Hal ini menegaskan bahwa fenomena tersebut bukan hanya isu hukum, tetapi juga kegagalan etika profesi yang mendasar. Kedua, regulasi hukum di Indonesia masih memiliki celah normatif yang signifikan. Meskipun UU ITE, UU TPKS, UU PDP, dan UU Pornografi dapat digunakan, belum ada aturan yang secara spesifik mengatur penyalahgunaan *AI*, sehingga menimbulkan kendala pembuktian, tumpang tindih norma, dan risiko reviktimisasi korban. Ketiga, terdapat research gap dalam literatur Indonesia terkait integrasi kode etik profesi TI internasional dengan konteks lokal dalam analisis *deepfake harassment*. Penelitian ini mengisi celah tersebut melalui analisis integratif sekaligus menawarkan rekomendasi operasional bagi profesional TI dalam tiga aspek: teknis, kelembagaan, dan kebijakan.

Untuk penelitian selanjutnya, disarankan dilakukan studi empiris yang mengukur tingkat pemahaman profesional TI di Indonesia terhadap kode etik profesi dalam konteks teknologi *AI*, serta studi perbandingan regulasi *deepfake* antara Indonesia dan negara-negara yang telah memiliki kerangka hukum *AI* yang lebih komprehensif. Pembaruan kode etik profesi TI oleh organisasi profesi nasional yang secara eksplisit mengakomodasi tantangan *deepfake* juga merupakan agenda mendesak yang perlu segera ditindaklanjuti.

DAFTAR PUSTAKA

[1] Fitri, D., Hidayah, A. N., Putri, A., Tanjung, N. H., & Izzati, S. (2025). Deepfake dan krisis kepercayaan: Analisis hukum terhadap penyebaran konten palsu di media sosial. *Jurnal Intelek Insan Cendikia, 2*, 11556–11568.

[2] Erdiyanti, N. L. P. D., Dinar, I. G. A. A. G. P., & Wirawan, A. (2026). Perlindungan hukum terhadap korban sexual harassment akibat manipulasi konten digital berbasis artificial intelligence. *Al-Zayn: Jurnal Ilmu Sosial dan Hukum, 4*, 3915–3924. https://doi.org/10.61104/alz.v4i2.4879

[3] Leliana, I., Irhamdika, G., Haikal, A., Septian, R., & Kusnadi, E. (2023). Etika dalam era deepfake: Bagaimana menjaga integritas komunikasi. *Jurnal Visi Komunikasi, 22*(2), 234–243. https://doi.org/10.22441/visikom.v22i02.24229

[4] Zahro, A., Fadhilah, R. R., Hermawati, S. Z., Imaduddin, G. N., & Santoso, A. L. (2024). Dampak penyalahgunaan deepfake dalam memanipulasi visual: Menguak potensi infopocalypse di era post-truth terhadap asumsi masyarakat pada media massa. *Jurnal Kawistara, 14*(3), 11–12. https://doi.org/10.22146/kawistara.98339

[5] Huwaida, F. S., Widodo, S., & Elviani, U. (2025). Deepfake di era digital: Tantangan tata keamanan siber dan tata kelola AI. *Jurnal Pendidikan Teknologi dan Komunikasi, 5*, 664–672.

[6] Rambe, N. U., Khoiri, N., & Qarai, W. (2024). Etika komunikasi di media sosial TikTok untuk mengantisipasi fenomena bullying. *Jurnal Manajemen Akuntansi, 4*(1), 133–138. https://doi.org/10.36987/jumsi.v4i1.4753

[7] Seveney, M. C., Wicaksono, D. B., & Soetijono, I. K. (2025). Urgensi regulasi terhadap penyalahgunaan deepfake berbasis artificial intelligence pada konten pornografi. *Disiplin: Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda, 31*(2), 97–106.

[8] Quratuainniza, H. S., & Nurkhaerani, E. (2025). Regulasi kecerdasan buatan untuk mengatasi penyalahgunaan deepfake di Indonesia. *Jurnal Politik, Sosial, Hukum dan Humaniora, 4*. https://doi.org/10.59246/aladalah.v2i4

[9] Risno, R., Kamarudin, K., & Dagani, K. (2021). Pertanggungjawaban pidana terhadap pelaku deepfake pornography. *Jurnal Tana Mana, 2*(1), 46–48. https://ojs.staialfurqan.ac.id/jtm/article/download/736/452/

[10] De Ruiter, A. (2021). The distinct wrong of deepfakes. *Philosophy & Technology*. https://doi.org/10.1007/s13347-021-00459-2

[11] Alexander, S. (2025). Deepfake cyberbullying: The psychological toll on students and institutional challenges of AI-driven harassment. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas, 98*(2), 36–50. https://doi.org/10.1080/00098655.2025.2488777

[12] Balmaceda, T., Belli, L. F., & Pérez, D. I. (2025). Deepfakes como actos comunicativos: Desafíos éticos sobre consentimiento y privacidad. *Trilogía Ciencia Tecnología Sociedad*. https://doi.org/10.22430/21457778.3684

[13] Ali, M., Fernando, Z. J., Huda, C., & Mahmutarom. (2024). Deepfakes and victimology: Exploring the impact of digital manipulation on victims. *Substantive Justice International Journal of Law*. https://doi.org/10.56087/substantivejustice.v8i1.306

[14] Noviantama, D., & Rahman, A. A. (2025). Deepfake: A review from the victimology perspective. *Contemporary Issues in Criminal Law*.
[15] Rini, R., & Cohen, L. (2022). Deepfakes, deep harms. *Journal of Ethics and Social Philosophy*.