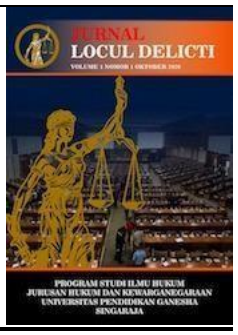
JURNAL LOCUS DELICTI

Volume 4 Nomor 2, Oktober 2023
p-ISSN:2723-7427, e-ISSN: 2807-6338
Open Access at : https://ejournal2.undiksha.ac.id/index.php/JLD
Program Studi Ilmu Hukum
Fakultas Hukum dan Ilmu Sosial
Universitas Pendidikan Ganesha Singaraja



ANALISIS YURIDIS TERHADAP PENYALAHGUNAAN KECERDASAN BUATAN DALAM PENIPUAN BERMODUS PENCULIKAN ANAK MELALUI IMITASI SUARA

Gede Eka Sidi Artama [1] dan Ni Putu Ega Parwati[2]

Universitas Pendidikan Ganesha[1], Universitas Pendidikan Ganesha[2]

E-mail : eka.sidi@student.undiksha.ac.id [1], ni.putu.ega.parwati@undiksha.ac.id [2]

Info Artikel

Masuk: 19 Mei 2023

Diterima: 27 Juli 2023

Terbit: 1 Oktober 2023

Keywords:

Artificial Intelligence, Fraud, Child Abduction Criminal Law, Regulation

Kata kunci:

Kecerdasan Buatan, Penipuan, Imitasi Suara, Regulasi

Abstract

This study aims to analyze the misuse of artificial intelligence (AI) in fraud cases with child abduction mode through voice imitation and the criminal responsibility of the perpetrators. The research method used is normative, focusing on the analysis of norms in the Criminal Code (KUHP) and the ITE Law relevant to criminal acts of fraud and technology abuse. The results of the study indicate that there is vagueness and legal vacuum in the regulation regarding the misuse of AI for fraud. Article 378 of the Criminal Code can be applied, but further interpretation is needed to effectively ensnare the perpetrators. More specific regulatory updates are needed to address AI-based crimes

Abstrak

Penelitian ini bertujuan untuk menganalisis penyalahgunaan kecerdasan buatan (AI) dalam kasus penipuan bermodus penculikan anak melalui imitasi suara serta pertanggungjawaban pidana terhadap pelaku. Metode penelitian yang digunakan adalah penelitian hukum normatif, dengan fokus pada analisis norma dalam KUHP dan UU ITE yang relevan terhadap tindak pidana penipuan dan penyalahgunaan teknologi. Hasil penelitian menunjukkan adanya kekaburan dan kekosongan hukum dalam pengaturan mengenai penyalahgunaan AI untuk penipuan. Pasal 378 KUHP dapat diterapkan, namun perlu interpretasi lebih lanjut untuk menjerat pelaku secara efektif. Pembaruan regulasi yang lebih spesifik dibutuhkan untuk mengatasi kejahatan berbasis AI.

Corresponding Author:
Gede Eka Sidi Artama
E-mail :
eka.sidi@student.undiksha.ac.id

Pendahuluan

Teknologi *Artificiall Intelligence* (AI) adalah salah satu bentuk kemajuan teknologi yang memiliki kemampuan untuk berpikir secara mandiri. AI dirancang untuk meniru proses berpikir dan pengambilan keputusan yang biasanya dilakukan oleh manusia, memungkinkan mesin untuk melakukan tugas-tugas kompleks dengan efisiensi yang tinggi (Kurniawan, 2023). Kecerdasan buatan (AI) telah membawa manfaat besar di berbagai bidang, namun juga membawa tantangan baru dalam hal keamanan dan privasi. Salah satu ancaman yang ditimbulkan adalah eksploitasi metode baru untuk melakukan penipuan penculikan anak melalui peniruan vokal (Yusnita, 2023). Teknologi AI memungkinkan pihak-pihak jahat untuk menciptakan suara yang sangat mirip dengan suara manusia sebenarnya yang dapat dieksploitasi untuk menciptakan situasi menakutkan atau memanipulasi orang tua dan anggota keluarga untuk membayar uang tebusan atau membuat mereka mengambil tindakan tertentu.

Dewasa ini, jagat maya digembarkan dengan kemunculan suara super realistis yang dibuat oleh teknologi yang dikenal dengan *Artificial Intelligence.* Bukti dari hal ini terlihat melalui munculnya laporan kasus yang terkait dengan hal tersebut yakni pada April 2023 dimana Seorang ibu di Arizona, AS, bernama Jennifer DeStefano nyaris menjadi korban kejahatan yang melibatkan kecerdasan buatan (AI). Pelaku menggunakan

teknologi tersebut untuk meniru suara anaknya, menciptakan situasi palsu seolah-olah anaknya telah diculik. Teknologi ini mampu mengenali serta meniru kehalusan, intonasi, dan pola bicara manusia dengan menggunakan algoritma pembelajaran mesin yang canggih. Proses kloning suara AI dimulai dengan mengumpulkan data suara dari target, seperti rekaman percakapan, wawancara, atau sumber audio lainnya. Setelah data terkumpul, algoritma pembelajaran mesin menganalisis dan mengidentifikasi pola unik dalam suara tersebut (Alviani & Fitri, 2024).

Dari kasus ini, tekonologi berupa AI dapat digunakan untuk membuat suara yang mirip dengan anak dari Jennifer DeStefano, sehingga membuat korban yakin bahwa ia sedang berkomunikasi langsung dengan anaknya. Cara kerja AI tersebut menjadi sangat berbahaya jika sampel suara yang digunakan berasal dari sumber yang tidak dapat dipertanggungjawabkan. Hal ini diperburuk oleh lemahnya regulasi perlindungan data pribadi, yang masih terfragmentasi dalam berbagai peraturan hukum terpisah dan cenderung hanya memberikan gambaran umum tentang konsep perlindungan data pribadi (Tampi et al., 2025).

Fenomena tersebut menjadi bagian dari kejahatan siber (*cyber crime*), yaitu tindak kriminal yang dilakukan oleh individu atau kelompok dengan memanfaatkan komputer dan alat telekomunikasi lainnya. Pelaku yang memiliki kemampuan dalam mengoperasikan komputer, seperti operator, programmer, analis, manajer, atau kasir, dapat melakukan kejahatan ini (Buçaj & Idrizaj, 2025). Tindakan yang dilakukan meliputi perusakan data, pencurian data, hingga penggunaan data secara ilegal. Perkembangan pesat teknologi komunikasi, seperti telepon, ponsel, dan alat telekomunikasi lainnya, yang terintegrasi dengan kemajuan teknologi komputer, menjadi faktor utama yang mendorong meningkatnya kasus *cyber crime* (Wibowo & Yulianingsih, n.d.).

Komputer dan internet menyediakan akses yang mudah dan cepat ke berbagai informasi, baik yang sah maupun yang tidak sah. Teknologi ini juga mempermudah pelaku untuk menyembunyikan identitas mereka, melacak jejak digital korban, dan menciptakan sarana untuk menjangkau target secara luas tanpa batas geografis. Alat-alat komunikasi modern memungkinkan pelaku untuk melakukan kejahatan dari jarak jauh, menjadikannya lebih sulit untuk dilacak dan diadili. Perkembangan teknologi juga memberikan pelaku *cyber crime* berbagai metode baru untuk melakukan tindakan kejahatan. Misalnya, penggunaan phishing untuk mencuri data pribadi seperti nomor kartu kredit atau akun bank, ransomware untuk mengunci data korban dan meminta tebusan, serta serangan denial-of-service yang bertujuan untuk membuat situs web atau sistem offline. Semua tindakan ini menunjukkan bahwa kejahatan *cyber* tidak hanya terbatas pada pencurian data atau uang, tetapi juga dapat memiliki dampak yang lebih luas, termasuk kerusakan reputasi, gangguan operasional bisnis, dan ancaman terhadap keamanan nasional.

Penelitian sebelumnya telah menunjukkan bahwa aturan hukum Indonesia masih memiliki banyak kesenjangan mengenai kejahatan kriminal teknologi kecerdasan buatan (AI) dalam *phishing* suara melalui ponsel. Sebuah studi oleh Alya Alviani dan Yenny Fitri Z. (2024) menunjukkan bahwa Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) tidak secara khusus mengatur mode kejahatan berbasis AI. Walaupun Pasal 28 ayat (1) Jo. Pasal 45A dari UU ITE dapat digunakan untuk mengurangi jumlah pelaku, Ketentuan ini secara eksplisit tidak termasuk teknologi AI yang lebih menuntut. Studi ini juga menemukan bahwa sebagian besar insiden *voice phising* di Indonesia mempengaruhi teknologi AI antara tahun 2023 hingga 2024, tetapi penegakan hukum masih menghadapi tantangan besar terutama dalam bukti teknis.

Penelitian (ALSA, 2024) memfokuskan bahwasannya pelaku kejahatan sering memanfaatkan rekaman suara korban dari media sosial agar kloning suara mirip dengan aslinya. Metode ini bisa menyulitkan aparat penegak hukum untuk membuktikan unsur "kesengajaan" yang telah diatur di dalam KUHP.

Ancaman ini meningkatkan kompleksitas penegakan hukum karena memerlukan pemahaman yang lebih mendalam tentang bagaimana teknologi ini dapat digunakan untuk melemahkan keselamatan pribadi dan merugikan masyarakat. Dari sudut pandang hukum dan teknis, langkah-langkah pencegahan dan penegakan hukum yang efektif diperlukan untuk melawan penyalahgunaan AI dalam penipuan berbasis pemalsuan suara. Peraturan yang jelas dan kuat perlu diterapkan untuk melindungi privasi dan hak individu serta mencegah meningkatnya insiden kejahatan dunia maya AI.

Untuk mencegah terjadinya masalah serupa pada Indonesia, diharapkan langkah-langkah proaktif. Pertama, perlu terdapat penyusunan regulasi yg tegas tentang penggunaan AI, khususnya yg berkaitan menggunakan proteksi data eksklusif & kebebasan berbicara.Undang-undang yg terdapat perlu diperbarui buat meliputi potensi penyalahgunaan AI pada penipuan, & perlu terdapat pengaturan yg ketat terhadap teknologi kloning suara.Kedua, krusial buat menaikkan literasi digital warga supaya bisa mengenali potensi ancaman & melaporkan insiden-insiden yg mencurigakan pada otoritas terkait.Selain itu, perlu adanya kampanye publik mengenai bahayanya kejahatan siber yg melibatkan AI buat menaikkan pencerahan akan risiko & pentingnya melindungi diri secara online.Ketiga, kolaborasi internasional pula diharapkan buat membuatkan keterangan & pengalaman pada menangani masalah- masalah serupa, dan memperkuat koordinasi pada penegakan aturan terhadap kejahatan siber yg memakai AI.Melalui langkah-langkah ini, dibutuhkan Indonesia bisa meminimalkan potensi ancaman &

melindungi warga berdasarkan penyalahgunaan kecerdasan protesis pada masa depan.

Berdasarkan uraian di atas, penelitian ini bertujuan untuk mengkaji dan menjawab beberapa pertanyaan kunci, yakni (1) bagaimana bentuk penyalahgunaan kecerdasan buatan (*Artificial Intelligence)* dalam kasus penipuan bermodus penculikan anak melalui imitasi suara? Dan (2) Bagaimana pertanggungjawaban pidana terhadap pelaku penyalahgunaan kecerdasan buatan dalam kasus penipuan bermodus penculikan anak?

Untuk menjawab pertanyaan-pertanyaan tersebut, penelitian ini menggunakan metode penelitian hukum normatif yang bertujuan menganalisis norma-norma hukum yang mengatur tindak pidana penipuan dan penyalahgunaan teknologi kecerdasan buatan dalam kejahatan siber, khususnya terhadap kekaburan dan kekosongan norma. Kekaburan terlihat pada ketidakjelasan pengaturan penggunaan AI dalam modus penipuan, sedangkan kekosongan muncul akibat belum adanya aturan spesifik terkait penyalahgunaan teknologi tersebut. Bahan hukum primer yang dikaji meliputi Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), dengan fokus pada Pasal 378 KUHP serta Pasal 32 ayat (2) dan Pasal 33 UU ITE. Analisis deduktif dilakukan untuk menghubungkan norma-norma hukum tersebut dengan fenomena penyalahgunaan teknologi dalam kejahatan siber sekaligus mengidentifikasi kekaburan dan kekosongan norma yang dapat menimbulkan ketidakpastian hukum, sehingga membuka peluang rekomendasi pembaruan regulasi di era digital dalam hukum pidana.

Pembahasan

A. Bentuk Penyalahgunaan Kecerdasan buatan (AI) dalam Kasus Penipuan Bermodus Penculikan Anak melalui Imitasi Suara

Bentuk penyalahgunaan kecerdasan buatan (AI) dalam kasus penipuan bermodus penculikan anak melalui imitasi suara semakin mengkhawatirkan di era digital saat ini. Teknologi AI yang semakin canggih memungkinkan pelaku untuk memanipulasi suara dengan sangat meyakinkan, menciptakan salinan suara seseorang yang terdengar persis seperti orang asli. Dalam skenario penipuan ini, pelaku dapat menggunakan AI untuk membuat pesan suara yang terdengar seperti orang tua atau kerabat dari anak yang diklaim telah diculik, meminta uang tebusan atau meminta bantuan. Keahlian AI dalam pemrosesan suara ini mempermudah pelaku untuk menciptakan suasana panik dan tekanan emosional pada target, memperdaya mereka untuk memberikan informasi pribadi atau uang yang diinginkan oleh penipu. Ancaman ini tidak hanya merusak kepercayaan dalam komunikasi suara, tetapi juga menimbulkan tantangan besar bagi penegakan hukum yang berupaya melacak pelaku dan melindungi korban.

Penyalahgunaan AI dalam penipuan semacam ini meningkatkan kompleksitas dalam penegakan hukum karena memerlukan pemahaman yang lebih mendalam tentang teknologi ini dan cara kerja teknik manipulasi suara. Pelaku dapat memanfaatkan kemampuan AI untuk menciptakan pesan suara yang sangat meyakinkan dan terdengar persis seperti orang yang dikenal oleh korban, seperti orang tua atau kerabat. Hal ini membuat korban lebih rentan terhadap penipuan, memperdaya mereka untuk mengikuti permintaan tanpa curiga. Tantangan ini lebih besar karena pelaku dapat menyembunyikan identitas mereka dengan lebih mudah menggunakan teknologi yang sulit dilacak. Penegak hukum harus menghadapi kesulitan dalam memverifikasi keaslian pesan suara dan mengidentifikasi pelaku di balik serangan tersebut. Selain itu, AI memungkinkan

pelaku untuk menciptakan suasana tekanan emosional pada korban, menambah kesulitan dalam menanggapi ancaman ini secara efektif.

Salah satu bentuk kejahatan yang marak memanfaatkan teknologi AI adalah penipuan. Hal ini didukung oleh kemampuan AI yang sangat canggih, seperti mempelajari pola dan meniru perilaku manusia secara detail. AI memungkinkan pelaku kejahatan membuat video atau rekaman suara yang sulit dideteksi sebagai palsu. Selain itu, kemudahan akses terhadap AI semakin memperbesar risiko penipuan, karena beberapa AI dapat dengan mudah menganalisis data pribadi seseorang, yang kemudian disalahgunakan untuk keuntungan pribadi oleh pihak yang tidak bertanggung jawab.

Kemampuan AI dalam memanipulasi data, termasuk identitas dan informasi, seringkali didasarkan pada dua mekanisme utama. Pertama, mekanisme *Natural Language Processing* (NLP), yang dapat menghasilkan teks menyerupai gaya penulisan manusia. Mekanisme ini memungkinkan pelaku membuat pesan phishing atau informasi palsu dengan tingkat akurasi tinggi yang sulit dideteksi. NLP juga digunakan untuk menganalisis emosi, opini, menerjemahkan bahasa, dan bahkan menarik informasi dari teks. Kedua, mekanisme *Generative Adversarial Networks* (GANs), yang digunakan untuk menciptakan konten palsu, seperti video, gambar, dan audio. GANs memungkinkan pelaku membuat identitas palsu, merekayasa peristiwa, hingga memanipulasi pasar, seperti harga saham atau cryptocurrency.

Meskipun AI membuka peluang tak terbatas untuk kemajuan, ia juga memperkenalkan risiko baru, khususnya dalam bentuk penipuan. Peningkatan risiko ini tidak hanya dipengaruhi oleh perkembangan teknologi yang pesat, tetapi juga oleh kurangnya kesiapan sumber daya manusia dalam memahami dan

mengelola teknologi AI. AI, yang memberikan efisiensi dan kemudahan, dapat menjadi bencana jika penggunaannya tidak terkendali dengan baik.

B. Pertanggungjawaban Pidana terhadap Pelaku Penyalahgunaan Kecerdasan Buatan dalam Kasus Penipuan Bermodus Penculikan Anak

Penipuan suara berbasis AI memanfaatkan teknologi kecerdasan buatan untuk meniru suara seseorang. Dengan menggunakan algoritme pembelajaran mendalam, suara dapat direplikasi dengan sangat akurat, membuat panggilan palsu terdengar seperti asli. Teknologi ini dimanfaatkan oleh penipu untuk menipu individu agar memberikan informasi sensitif atau mentransfer uang.

Istilah "penipuan" berakar dari kata "tipu," yang merujuk pada tindakan menipu, berbohong, memalsukan, atau perilaku serupa lainnya yang bertujuan untuk menyesatkan, mengecoh, atau memperoleh keuntungan. Setiap bentuk penipuan yang merugikan pihak lain dianggap melanggar hukum dan dapat menimbulkan konsekuensi hukum (Alviani & Fitri, 2024).

Tindak pidana penipuan telah diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP), yang menyatakan:

"Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan menggunakan nama palsu atau martabat palsu; dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun."

Dalam kasus penipuan bermodus penculikan anak menggunakan kecerdasan buatan (AI), pelaku memanfaatkan teknologi untuk meniru suara korban anak dan

mengelabui orang tua atau wali dengan narasi bahwa anak mereka diculik. Pelaku kemudian menuntut tebusan dalam bentuk uang. Modus operandi ini melibatkan rangkaian kebohongan dan tipu muslihat, yang bertujuan untuk mendapatkan keuntungan secara melawan hukum, sehingga memenuhi unsur-unsur tindak pidana penipuan sebagaimana diatur dalam Pasal 378 KUHP.

Sementara itu, Pasal 28 Ayat (1) UU ITE mengatur penyebaran berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. Namun, penerapan pasal ini menghadapi kendala karena orang tua korban bukan konsumen dalam transaksi elektronik, dan informasi yang disebarkan oleh pelaku tidak terkait dengan sistem transaksi elektronik yang dimaksud dalam UU ITE.

Permasalahan hukum muncul karena meskipun pelaku jelas melakukan kejahatan dengan memanfaatkan teknologi AI, regulasi yang ada belum secara spesifik mencakup kejahatan seperti ini, sehingga terdapat kekosongan hukum. Oleh karena itu, diperlukan interpretasi yang mengintegrasikan Pasal 378 KUHP dan Pasal 28 Ayat (1) UU ITE. Pasal 378 KUHP tetap menjadi dasar hukum utama untuk menjerat pelaku karena unsur-unsurnya terpenuhi dalam tindakan penipuan tersebut. Sementara itu, Pasal 28 Ayat (1) UU ITE dapat diperluas melalui interpretasi hukum untuk mencakup tindakan menyebarkan informasi palsu atau menyesatkan yang tidak selalu dalam konteks transaksi elektronik.

Untuk memastikan pelaku kejahatan serupa dapat dihukum, perlu dilakukan pembaruan regulasi yang secara eksplisit mengatur penyalahgunaan teknologi AI dalam tindak pidana, termasuk kejahatan yang melibatkan manipulasi suara atau

data. Selain itu, definisi "konsumen" dalam UU ITE perlu diperluas agar mencakup pihak-pihak yang dirugikan dalam transaksi berbasis teknologi meskipun tidak terjadi jual beli. Dengan langkah-langkah tersebut, penegakan hukum dapat lebih efektif melindungi masyarakat dari ancaman kejahatan berbasis teknologi di masa depan.

Dalam konteks perlindungan data pribadi, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan tonggak penting dalam menjawab tantangan era digital. Undang- undang ini bertujuan untuk memberikan jaminan privasi individu dan data pribadi, termasuk perlindungan terhadap potensi ancaman dari teknologi kecerdasan buatan (AI). Salah satu ketentuan terpenting dalam UU PDP adalah pembentukan Kantor Perlindungan Data (LOPDP) yang bertugas memastikan pelaksanaan UU ini berjalan sesuai aturan yang diatur dalam Pasal 58. LOPDP didirikan berdasarkan keputusan presiden dan berperan strategis dalam mengatasi berbagai permasalahan terkait, termasuk teknologi maju seperti AI.

Di era digital yang penuh inovasi, penggunaan AI untuk memproses data pribadi menghadirkan berbagai peluang dan tantangan. Meskipun AI mampu melakukan analisis data berskala besar dan sangat efisien, AI juga membawa risiko penyalahgunaan data pribadi untuk tujuan berbahaya seperti manipulasi data dan pengambilan keputusan yang bias. Dengan perkembangan ini, UU PDP memberikan kerangka hukum penting untuk mengatur penggunaan teknologi AI dalam pemrosesan data. Peraturan ini bertujuan untuk memastikan data pribadi tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.

Mengingat UU PDP tidak hanya memuat ketentuan administratif dan sanksi atas

pelanggaran, namun juga menekankan pentingnya kerja sama antara pemerintah, lembaga penegak hukum, perusahaan swasta, dan pelaku industri digital. Dalam konteks AI, kolaborasi ini menjadi semakin penting, terutama dalam mendorong pengembangan teknologi yang beretika dan transparan. Selain itu, edukasi masyarakat melalui media massa juga diperlukan untuk meningkatkan kesadaran akan pentingnya menghormati hak privasi dan data pribadi. Dengan mengambil langkah-langkah terpadu, kita dapat meminimalkan risiko penyalahgunaan teknologi, termasuk melalui AI, dan menciptakan lingkungan digital yang aman dan tepercaya.

Kolaborasi lintas sektor ini tidak hanya bertujuan untuk menegakkan perlindungan hukum bagi pemilik data pribadi, tetapi juga untuk mengembangkan infrastruktur digital yang lebih inklusif dan tangguh. Pemerintah, misalnya, memiliki peran strategis dalam menyusun kebijakan yang tidak hanya mencegah penyalahgunaan data pribadi, tetapi juga mendorong inovasi yang bertanggung jawab. Kebijakan ini dapat mencakup peraturan tentang transparansi pengolahan data, kewajiban pelaporan insiden keamanan data, serta pembentukan lembaga pengawas independen yang bertugas mengawasi implementasi UU PDP secara efektif.

Di sisi lain, perusahaan swasta dan pelaku industri digital juga memegang tanggung jawab besar dalam memastikan bahwa teknologi yang mereka kembangkan dan gunakan tidak hanya inovatif, tetapi juga mematuhi prinsip-prinsip etika dan regulasi yang berlaku. Hal ini mencakup adopsi teknologi berbasis kecerdasan buatan (AI) yang transparan, non-diskriminatif, dan menghormati hak privasi pengguna. Perusahaan harus melakukan audit berkala

terhadap algoritma mereka untuk mendeteksi potensi bias, memastikan keadilan dalam proses pengambilan keputusan otomatis, serta memberikan informasi yang jelas kepada pengguna tentang bagaimana data mereka dikelola.

Dalam konteks kecerdasan buatan, kebutuhan akan pengaturan dan pengawasan yang ketat menjadi semakin penting mengingat potensi dampaknya yang luas, baik secara sosial maupun ekonomi. Teknologi AI dapat meningkatkan efisiensi dan produktivitas, tetapi juga dapat menjadi ancaman jika digunakan untuk tujuan yang melanggar hukum atau etika. Oleh karena itu, pengembangan AI yang beretika harus menjadi prioritas, didukung oleh regulasi yang jelas, kolaborasi lintas sektor, dan komitmen dari semua pihak yang terlibat.

Aspek edukasi juga menjadi salah satu elemen penting dalam penerapan UU PDP. Masyarakat perlu diberikan pemahaman yang memadai mengenai pentingnya menjaga privasi dan melindungi data pribadi mereka, baik melalui kampanye nasional, seminar, lokakarya, maupun melalui media sosial dan media massa. Edukasi ini harus mencakup informasi praktis tentang cara melindungi data pribadi, mengenali ancaman siber seperti phishing dan malware, serta meningkatkan literasi digital agar masyarakat dapat lebih waspada terhadap risiko yang ada di dunia maya.

Selain itu, lembaga penegak hukum harus terus memperbarui kemampuan mereka dalam menangani kejahatan siber dan pelanggaran privasi data yang semakin kompleks. Hal ini mencakup pelatihan teknis, penguatan kerja sama internasional dalam menangani kasus lintas batas, serta pengembangan alat dan teknologi pendukung untuk menyelidiki dan menindak pelanggaran yang melibatkan data pribadi.

Kesimpulan

Penyalahgunaan *Artificial Intelligence* (AI) dalam kasus penipuan bermodus penculikan anak melalui imitasi suara merupakan ancaman serius di era digital. Teknologi AI memungkinkan pelaku untuk menciptakan suara palsu yang sangat meyakinkan, sehingga korban percaya sedang berinteraksi dengan orang yang dikenal. Tindakan ini diperparah oleh lemahnya regulasi terkait perlindungan data pribadi dan penggunaan AI, yang menimbulkan kekaburan dan kekosongan hukum.

Meskipun Pasal 378 KUHP tentang penipuan dapat diterapkan, interpretasi yang lebih luas diperlukan untuk menjerat pelaku secara efektif. UU ITE, khususnya Pasal 28 Ayat (1), kurang relevan karena tidak secara spesifik mengatur penipuan semacam ini. Untuk itu, diperlukan pembaruan regulasi yang secara eksplisit mengatur penyalahgunaan AI dalam tindak pidana, termasuk manipulasi suara, serta memperluas definisi "konsumen" dalam UU ITE agar mencakup korban penipuan yang tidak terlibat dalam transaksi elektronik. Langkah-langkah ini penting untuk memperkuat penegakan hukum dan melindungi masyarakat dari ancaman kejahatan berbasis teknologi di masa depan.

DAFTAR PUSTAKA

Buku:

Idik Saeful Bahri. (2020). *Cyber Crime Dalam Sorotan Hukum Pidana* (Vol. 159). Bahasa Rakyat.

Sirait, T. M., (2024). *Cyber Law dalam Teori dan Perkembangannya (Cyber Crime, Privacy Data, E- Commerce)*. Deepublish.

Peraturan Perundang-Undangan

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Jurnal dan Publikasi Ilmiah

Alviani, A. (2024). Legal Regulations On Criminal Acts Against Misuse Of Ai (Artificial Intelligence) Technology In Voice Phishing Fraud Via Mobile Phones. *Jurnal Hukum De'rechtsstaat*, *10* (2), 207-216.

Amelia, Y. F., Kaimuddin, A., & Ashsyarofi, H.L. (2024). Pertanggungjawaban Pidana Pelaku Terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake Menurut Hukum Positif Indonesia. *Dinamika*, *30* (1), 9675-9691.

Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, *8*(1). https://doi.org/10.31893/multirev.2025024

Hapriyanto, A. R. (2023). The Urgency of Adopting Regulations on Artificial Intelligence Utilization to Enhance Personal Data Protection in Indonesia. *Asian Journal of Engineering, Social and Health*, *2*(12), 1581-1587.

Kurniawan, A. (2023). Pengembangan E-Modul Berbasis Android Menggunakan Teknologi Ai (Artificial Intelligence) Pada Materi Media Dan Produksi. *DEVOSI Jurnal Teknologi Pembelajaran*, *13*(2), 27–34.

Novera, O. (2024). Analisis Pengaturan Hukum Pidana terhadap Penyalahgunaan Teknologi Manipulasi Gambar (Deepfake) dalam Penyebaran Konten Pornografi Melalui Akun Media Sosial. *El-Faqih: Jurnal Pemikiran dan Hukum Islam*, ALSA, U. (2024). *Urgensi Pengaturan AI Di Indonesia*. https://www.alsalcunsri.org/post/urgensi-pengaturan-ai-di-indonesia

Sitompul, F., Manik, A. P. P., Sinaga, C. D.,

Purba, A. T., & Satria, A. (2024). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Hukum Indonesia. *Jaksa: Jurnal Kajian Ilmu Hukum Dan Politik*, *2*(2), 222-

228.

Sutarli, A. F., & Kurniawan, S. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia. *Innovative: Journal Of Social Science Research*, *3*(2), 4208-

4221.

Tampi, J. M., Mohede, N., & Wongkar, V. A. (2025). *Tinjauan Yuridis Terhadap Pelanggaran Privasi Berdasarkan Uu No 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Studi Kasus Tokopedia)*. *13*(1).

Wibowo, G., & Yulianingsih, S. (n.d.). *Teknologi informasi* (J. T. Santoso (ed.)). Yayasan Prima Agus Teknik.

Yusnita, W. (2023). Hati-Hati! Penipuan Bermodus Culik Anak Dibantu Teknologi AI. *Detikinet*. https://inet.detik.com/cyberlife/d-6684495/hati-hati-penipuan-bermodus-culik-anak-dibantu-teknologi-ai

10(2), 460-474.