

**ANALISIS HUKUM ATAS TINDAK PIDANA PENIPUAN MELALUI
REKAMAN SUARA BERBASIS KECERDASAN BUATAN (AI) DALAM
PERSPEKTIF KEJAHATAN EKONOMI**
*LEGAL ANALYSIS OF FRAUD CRIMES THROUGH ARTIFICIAL
INTELLIGENCE (AI)-BASED VOICE RECORDINGS FROM AN
ECONOMIC CRIME*

Richo Ardi Darmawan, Ahmad Irzal Fardiansyah dan Fristia Berdian Tamza

Korespondensi Penulis : richodarmawan77@gmail.com ahmad.irzal@fh.unila.ac.id,
fristia.berdia@fh.unila.ac.id

Magister Ilmu Hukum, Fakultas Hukum, Universitas Lampung

Citation Structure Recommendation :

Darmawan, Richo Ardi, Ahmad Irzal Fardiansyah dan Fristia Berdian Tamza. *Analisis Hukum atas Tindak Pidana Penipuan melalui Rekaman Suara Berbasis Kecerdasan Buatan (AI) dalam Perspektif Kejahatan Ekonomi*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.7 (2025).

ABSTRAK

Penelitian ini menganalisis tindak pidana penipuan menggunakan rekaman suara berbasis kecerdasan buatan (AI) dalam kerangka kejahatan ekonomi. Perkembangan teknologi AI memungkinkan pelaku meniru suara individu untuk menipu korban, sehingga menimbulkan kerugian finansial dan tantangan hukum. Studi ini menggunakan pendekatan normatif dengan analisis peraturan perundang-undangan dan kasus aktual. Hasil menunjukkan bahwa ketentuan hukum saat ini belum cukup memadai untuk menangani modus baru ini secara spesifik. Kesimpulannya, diperlukan penyempurnaan hukum pidana yang responsif terhadap perkembangan teknologi.

Kata Kunci: Kejahatan Ekonomi, Kecerdasan Buatan, Penipuan, Rekaman Suara, Teknologi

ABSTRACT

Fraud through voice recordings based on artificial intelligence (AI) is increasingly widespread and causes significant economic losses. This study analyzes the legal aspects of such fraud crimes from the perspective of economic crime by reviewing existing regulations and law enforcement. The results indicate that current regulations are not fully capable of anticipating the development of AI technology in voice fraud. In conclusion, there is a need to improve regulations and adapt law enforcement to technology to effectively prevent and handle this crime.

Keywords: Artificial Intelligence, Economic Crime, Fraud, Voice Recording, Criminal Act

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah menciptakan banyak perubahan mendasar dalam berbagai aspek kehidupan manusia. Salah satu inovasi di era digital yang paling mencolok adalah kemunculan kecerdasan buatan (Artificial Intelligence/AI) dan aplikasinya dalam kehidupan sehari-hari¹. AI dirancang untuk mempermudah aktivitas manusia, meningkatkan efisiensi serta kualitas hidup, dan memberikan kemudahan di berbagai sektor, seperti industri, pendidikan, pelayanan publik, hingga hiburan. Namun, sebagaimana filsuf teknologi sering mengingatkan bahwa setiap inovasi membawa sisi gelap yang saling beradu dengan manfaatnya. AI telah menjadi pedang bermata dua memungkinkan munculnya modus kejahatan baru, salah satunya adalah penipuan melalui rekaman suara atau kloning suara yang sangat realistis melalui deep learning atau generative adversarial networks².

Pada perkembangan teknologi kecerdasan buatan (AI), terdapat perbedaan mendasar antara *de jure* dan *de facto* dalam penanganan kejahatan yang memanfaatkan teknologi ini, khususnya penipuan berbasis rekaman suara AI. *De jure*, atau hukum yang seharusnya berlaku, mengharuskan adanya aturan yang mengatur penggunaan teknologi ini dengan tepat, sehingga tindak pidana seperti penipuan melalui kloning suara dapat dihukum secara adil dan efektif. Namun, *de facto*, atau kenyataan yang ada di lapangan, menunjukkan bahwa regulasi yang ada belum cukup memadai untuk menangani fenomena ini.

Hukum pidana di Indonesia, seperti Pasal 378 Kitab Undang-Undang Hukum Pidana yang mengatur tentang penipuan, memang dapat diterapkan dalam kasus-kasus penipuan dengan menggunakan identitas palsu. Namun, *de facto*, teknologi AI yang memungkinkan kloning suara dan manipulasi data digital belum sepenuhnya diakomodasi. Hal ini menyebabkan ketidakjelasan dalam penerapan hukum terhadap pelaku yang memanfaatkan teknologi untuk menipu, mengingat teknologi berkembang lebih cepat daripada pembaruan hukum yang ada.

¹ Harry Surden, *Artificial Intelligence and Law: An Overview*, Georgia State University Law Review, Vol.35 (2019).

² Kirana Rukmayuninda Ririh dkk., *Studi Komparasi dan Analisis SWOT pada Implementasi Kecerdasan Buatan (Artificial Intelligence) di Indonesia*, Jurnal Teknik Industri, Vol.15, No.2 (2020).

Contoh kasus penipuan berbasis rekaman suara AI yang semakin marak adalah penipuan dengan kloning suara anggota keluarga yang dilakukan oleh pelaku menggunakan teknologi deepfake. Dalam beberapa kasus yang terlapor, pelaku berhasil menipu korban dengan mereplikasi suara keluarga yang terdengar sangat meyakinkan melalui rekaman suara yang hanya berdurasi beberapa detik. Misalnya, kasus yang terjadi pada tahun 2022, di mana seorang ibu melaporkan bahwa ia hampir mentransfer uang yang diminta oleh seseorang yang mengaku sebagai anaknya yang sedang dalam keadaan darurat. Setelah dilakukan penyelidikan, terungkap suara tersebut adalah hasil kloning menggunakan AI.

Kasus lainnya adalah penipuan yang terjadi di sektor perbankan, di mana suara yang dikloning digunakan untuk memanipulasi nasabah agar melakukan transfer uang ke rekening yang tidak sah. Kasus-kasus seperti ini menunjukkan bagaimana teknologi deepfake dapat digunakan untuk menipu, mengelabui, dan merugikan individu secara finansial dengan cara yang sangat sulit dideteksi tanpa pengawasan yang tepat. Fenomena penipuan berbasis rekaman suara AI ini semakin nyata seiring meningkatnya kualitas teknologi audio sintetis yang mampu meniru suara seseorang dengan sangat detail.³

Dengan algoritme pembelajaran mendalam, pelaku dapat mereplikasi suara, intonasi, hingga emosi dari target hanya melalui sample suara yang diperoleh secara daring, misalnya dari media sosial atau hasil percakapan singkat, bahkan hanya tiga hingga sepuluh detik rekaman suara asli sudah cukup untuk menghasilkan kloning suara yang meyakinkan. Penipu kemudian menggunakan kloning suara tersebut untuk melakukan berbagai tindakan manipulatif, seperti phishing suara, permintaan transfer dana, maupun interaksi palsu yang menyesatkan korban. Kasus yang sering terjadi meliputi korban menerima panggilan “darurat” menggunakan suara anggota keluarga yang telah diklon, sehingga mereka mudah tergerak untuk melakukan tindakan sesuai permintaan pelaku.⁴

³ M.M. Gede Priana Dwipratama, *Implikasi Kecerdasan Buatan dalam Industri Pertahanan : Tantangan dan Peluang bagi Indonesia*, diakses dari <https://www.kemhan.go.id/pohtan/2024/03/20/implikasi-kecerdasan-buatan-dalam-industri-pertahanan-tantangan-dan-peluang-bagi-indonesia.html>, diakses pada 18 Desember 2025.

⁴ Muhammad Tan Abdul Rahman Haris dan Tantimin, *Analysis of Criminal Law Liability for the Use of Artificial Intelligence in Indonesia*, Jurnal Komunikasi Hukum (JKH), Vol.8, No.1 (2022).

Secara filosofis, ancaman kejahatan inovasi teknologi merefleksikan dilema kemajuan manusia yang selalu diikuti risiko moral, sosial, maupun hukum. Sejarah kemunculan teknologi sejak mesin uap, listrik, hingga AI selalu berpotensi menciptakan “*disruptive effect*” terhadap tatanan etis dan legal yang ada. Dalam penipuan suara berbasis AI, pertanyaan kritis muncul: sejauh mana manusia dapat tetap mengendalikan teknologi agar tak berujung pada penyalahgunaan? Bagaimana pertanggungjawaban hukum dapat ditegakkan di tengah perkembangan teknologi yang berjalan lebih cepat dari regulasi? Kajian filosofis harus mempertimbangkan hakikat penipuan dalam ranah digital, di mana batas antara otentik dan palsu, nyata dan sintetis, semakin kabur seiring berkembangnya AI deepfake.⁵

Dari sisi yuridis, Indonesia hingga saat ini dihadapkan pada tantangan regulasi yang belum sepenuhnya mampu mengantisipasi modus kejahatan digital, khususnya deepfake dan penipuan suara AI. Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP) memang masih menjadi dasar penjeratan pelaku penipuan dengan menggunakan identitas palsu, namun dalam kasus rekaman suara berbasis AI, interpretasi hukum yang lebih komprehensif dibutuhkan agar hukum dapat menjawab perkembangan modus baru ini secara efektif. Demikian pula UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) memuat pasal terkait manipulasi data elektronik dan penipuan, namun belum mengatur secara spesifik penyalahgunaan AI maupun definisi otentisitas suara dan data audio.⁶

Analisis yuridis yang berkembang di literatur hukum mengidentifikasi adanya kekosongan norma dan ketidakjelasan regulasi terkait penyalahgunaan AI dalam tindak pidana, sehingga menimbulkan ketidakpastian hukum dan membuka celah eksploitasi oleh pelaku kejahatan siber. Perlindungan hukum terhadap korban juga masih bersifat parsial karena hak substansi seperti ganti rugi atau pelaporan sering terhambat oleh verifikasi digital dan identifikasi pelaku yang menggunakan teknologi untuk menyembunyikan jejak. Tantangan penegakan hukum inilah yang mendorong urgensi pembaruan regulasi agar hukum nasional dan internasional dapat responsif terhadap perkembangan modus penipuan berbasis AI.⁷

⁵ Saphalya Peta, *Journey of Artificial Intelligence Frontier: A Comprehensive Overview*, Global Journal of Computer Science and Technology, Vol.23, Issue 2 (2023).

⁶ Faizal Adi Surya, *Perlindungan Hukum Korban Kekerasan Seksual dalam Pemberitaan Media Online di Indonesia*, Jurnal Hukum Samudra Keadilan, Vol.17, No.1 (2022).

⁷ Made Sadika Pusdiana dkk., *Penegakan Hukum terhadap Tindak Pidana Penipuan dengan Modus Arisan Online pada Polres Nias*, Locus, Vol.2, No.11 (2023).

Kajian sosiologis atas kejahatan penipuan suara berbasis AI menunjukkan bahwa risiko sosial yang ditimbulkan tidak sebatas pada kerugian ekonomi, tetapi juga menimbulkan trauma psikologis dan kerentanan sosial baru di masyarakat digital. Masyarakat kerap menjadi korban karena minimnya literasi digital, rendahnya pengetahuan tentang modus deepfake, serta kepercayaan yang diberikan kepada pihak yang dianggap “terpercaya”. Data menunjukkan bahwa dalam lima tahun terakhir, terjadi peningkatan signifikan kasus penipuan digital yang berbasis audio dan video hoax, baik di media sosial maupun platform transaksi daring.⁸

Berbagai pihak mulai dari pemerintah, penegak hukum, akademisi, hingga platform teknologi sudah berupaya melakukan sosialisasi dan mitigasi, namun modus penipuan berbasis AI terus berevolusi, sehingga masyarakat harus meningkatkan kewaspadaan dan literasi teknologi agar tidak menjadi korban. Selain itu, pembaruan perangkat regulasi perlu dilakukan dalam bentuk penguatan cyberlaw, perlindungan data pribadi, hingga kerjasama lintas negara dalam penanganan penipuan digital berbasis AI. Negara harus mampu mengembangkan strategi hukum baru yang adaptif, mengingat AI deepfake dapat merusak reputasi individu, mengganggu stabilitas ekonomi, dan memanipulasi opini publik dengan skala yang lebih luas.⁹

Terdapat beberapa penelitian terdahulu yang relevan dengan topik penipuan berbasis AI, namun penelitian ini memiliki kebaruan yang menonjol. Penelitian seperti yang dilakukan oleh Afnan (2022) tentang "Perlindungan Hukum Penyalahgunaan Artificial Intelligence Deepfake pada Layanan Pinjaman Online" menyoroti aspek perlindungan hukum terhadap penyalahgunaan AI dalam pinjaman online, namun tidak membahas penipuan berbasis suara. Penelitian Haris dan Tantimin (2022) yang berfokus pada tanggung jawab hukum penggunaan kecerdasan buatan di Indonesia juga memberikan dasar bagi pemahaman hukum terhadap teknologi ini, namun tidak secara spesifik membahas penipuan yang melibatkan teknologi deepfake suara. Sementara itu, Ririh et al. (2020) dengan analisis SWOT terkait implementasi AI di Indonesia, dan Ramadhani (2022) yang membandingkan regulasi Indonesia dengan Artificial Intelligence Act Uni Eropa,

⁸ H.A. Afnan, *Perlindungan Hukum Penyalahgunaan Artificial Intelligence Deepfake pada Layanan Pinjaman Online*, Skripsi, Universitas Muhammadiyah Surakarta, Surakarta, 2022.

⁹ Dikdik M. Arief Mansur dan Elisatris, *Cyber Law Aspek Hukum Teknologi Informasi*, PT Refika Aditama, Bandung, 2009.

memberikan perspektif luas terkait perkembangan regulasi AI, namun belum menyoroti aspek penipuan berbasis suara. Penelitian ini memiliki kebaruan dengan memfokuskan pada penipuan yang memanfaatkan teknologi deepfake suara dan mengusulkan perlunya regulasi yang lebih spesifik dan adaptif untuk mengatasi masalah tersebut.

Kekosongan hukum yang ada terletak pada ketidakmampuan regulasi yang berlaku saat ini untuk mengakomodasi penipuan yang dilakukan dengan menggunakan teknologi AI, khususnya dalam hal kloning suara. Pasal 378 KUHP yang mengatur penipuan, meskipun bisa diterapkan dalam kasus penipuan umum, tidak secara spesifik mengatur modus penipuan yang melibatkan manipulasi suara berbasis AI. Begitu juga dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, meskipun mengatur tentang manipulasi data elektronik, tidak membahas secara rinci soal manipulasi data suara atau rekaman yang dihasilkan oleh teknologi AI. Hal ini menciptakan celah hukum yang memungkinkan pelaku kejahatan untuk memanfaatkan teknologi ini tanpa adanya sanksi yang jelas. Oleh karena itu, penting untuk mengembangkan regulasi baru yang lebih responsif terhadap perkembangan teknologi ini, dengan memberikan ketentuan yang lebih spesifik tentang penyalahgunaan AI dalam tindak pidana.

Penelitian ini berangkat dari kebutuhan akan perangkat hukum yang efektif untuk mengatur, mencegah, dan menegakkan hukum terhadap tindak pidana penipuan suara berbasis kecerdasan buatan yang kini tergolong kejahatan ekonomi berdampak luas. Perumusan topik dilakukan dengan mengkaji latar belakang filosofis, yuridis, dan sosiologis terkait fenomena penipuan suara AI, serta menjelaskan bagaimana regulasi saat ini belum cukup optimal menjerat pelaku dan melindungi korban. Dengan demikian, tujuan penelitian ini adalah melakukan analisis hukum secara mendalam atas tindak pidana penipuan melalui rekaman suara berbasis kecerdasan buatan (AI) dalam perspektif kejahatan ekonomi guna memberikan rekomendasi bagi pembaruan regulasi dan penegakan hukum adaptif di era digital.¹⁰

¹⁰ Fitria Ramadhani, *Kesenjangan Regulasi Kecerdasan Buatan di Indonesia: Analisis Komparatif dengan Artificial Intelligence Act Uni Eropa*, Legislasi Indonesia, Vol.20, No.1 (2022), p.77–91.

Judul penelitian “Analisis Hukum atas Tindak Pidana Penipuan melalui Rekaman Suara Berbasis Kecerdasan Buatan (AI) dalam Perspektif Kejahatan Ekonomi” merefleksikan tantangan hukum yang dihadapi saat perkembangan teknologi lebih cepat daripada respons regulasi. Penulisan ini ditujukan bagi pemerhati hukum, penegak hukum, pembuat kebijakan, akademisi, serta masyarakat umum yang ingin memahami secara holistik fenomena penipuan suara AI sebagai ancaman baru bagi keadilan dan keamanan ekonomi.

Rumusan masalah penelitian dapat dirumuskan dengan pertanyaan:

1. Bagaimana analisis hukum atas tindak pidana penipuan melalui rekaman suara berbasis kecerdasan buatan (AI) dalam perspektif kejahatan ekonomi?
2. Bagaimana analisis hukum atas tindak pidana penipuan melalui rekaman suara berbasis kecerdasan buatan (AI) dalam perspektif kejahatan ekonomi di Indonesia?

B. PEMBAHASAN

1. Tindak Pidana Penipuan Melalui Rekaman Suara Berbasis Kecerdasan Buatan (AI) dalam Perspektif Kejahatan Ekonomi

Secara filosofis, kemajuan kecerdasan buatan yang memungkinkan penciptaan rekaman suara yang sangat mendekati originalitas manusia menimbulkan dilema yang fundamental terkait nilai kebenaran, kepercayaan, dan otentisitas. Teknologi AI, khususnya deepfake voice, tidak hanya mengaburkan batas antara yang nyata dan yang palsu, tetapi juga mengancam fondasi moral dan etika yang selama ini menjadi pijakan hukum. Hal ini menyebabkan pertanyaan mendalam tentang bagaimana manusia dapat menjaga keadilan dan kepercayaan sosial kala teknologi dapat menipu indra dan akal manusia. Dalam kejahatan, penetrasi AI memberikan tantangan baru dalam membedakan antara fakta dan rekayasa, yang secara konseptual mengganggu prinsip dasar hukum pidana dan keamanan ekonomi masyarakat.¹¹

¹¹ Najwa Fathiro Cahyono, Khurrotul 'Uyun dan Siti Mukaromah, *Etika Penggunaan Kecerdasan Buatan pada Teknologi Informasi*, Prosiding Seminar Nasional Teknologi Dan Sistem Informasi, Vol.3, No.1 (2023).

Dari perspektif yuridis, permasalahan utama terletak pada ketidakjelasan regulasi yang secara khusus mengatur penyalahgunaan teknologi AI dalam tindak pidana penipuan. Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP) memberi dasar umum tentang penipuan, yakni tindakan memperdaya untuk memperoleh keuntungan yang merugikan pihak lain¹². Namun, keberadaan rekaman suara yang diproduksi secara artifisial ini memerlukan interpretasi kontekstual yang adaptif, mengingat teknologi tersebut belum secara eksplisit disebut dalam regulasi nasional. Selain itu, UU ITE menyediakan norma untuk menghadapi kejahatan di ranah elektronik, namun belum merinci mekanisme hukum untuk penipuan dengan menggunakan AI deepfake¹³. Kekosongan norma ini berpotensi menciptakan celah hukum, di mana perlindungan hukum terhadap korban menjadi terbatas akibat ketidakmampuan regulasi mengakomodasi teknologi yang cepat berkembang. Selain itu, pembuktian rekaman suara hasil AI sebagai alat bukti hukum masih menjadi perdebatan karena keterbatasan teknik forensik audio yang belum standar dan mapan di Indonesia. Permasalahan yuridis ini menjadi hambatan besar dalam penegakan hukum yang efektif, menyebabkan ketidakpastian hukum dan potensi manipulasi teknologi oleh pelaku kejahatan.

Secara sosiologis, penipuan suara menggunakan kecerdasan buatan membawa dampak yang tidak hanya bersifat ekonomi, tetapi juga sosial dan psikologis. Korban tidak hanya menderita kerugian materiil yang signifikan, namun juga mengalami tekanan psikologis akibat kebingungan identitas dan kecurigaan yang tumbuh di masyarakat. Hal ini berdampak pada menurunnya tingkat kepercayaan antar individu serta antara masyarakat dan institusi, yang pada gilirannya dapat mengganggu stabilitas sosial. Rendahnya literasi digital dan kurangnya kesadaran masyarakat terhadap modus operandi teknologi deepfake menyebabkan kerentanan yang tinggi terhadap kejahatan ini. Ketidaksiapan sosial dan minimnya edukasi menjadi faktor yang mempercepat penyebaran modus penipuan berbasis AI, sehingga diperlukan respon komprehensif yang melibatkan edukasi publik dan penguatan sistem hukum. Fenomena ini sekaligus menjadi refleksi perlunya penyesuaian norma sosial dan strategi mitigasi baru guna menghadapi transformasi teknologi yang membawa risiko sosial berskala besar.

¹² Pusat Pendidikan dan Pelatihan, *Azaz-Azaz Hukum Pidana*, PPPJ, Jakarta, 2010.

¹³ Afnan, *Op.Cit.*

Teori normatif hukum menekankan pentingnya hukum untuk mencapai keadilan sosial dan melindungi kepentingan umum. Dalam konteks penipuan berbasis teknologi AI, regulasi yang ada di Indonesia, seperti Pasal 378 KUHP dan UU ITE, masih bersifat umum dan belum mampu mengatasi kejahatan yang melibatkan teknologi canggih seperti deepfake. **Teori hukum progresif** menyarankan bahwa hukum harus selalu berkembang mengikuti dinamika sosial dan teknologi. Oleh karena itu, hukum pidana Indonesia perlu menyesuaikan diri dengan perkembangan teknologi AI agar dapat memberikan perlindungan yang efektif. Jika dibandingkan dengan regulasi di negara maju, seperti **AI Act** Uni Eropa, yang sudah mengatur secara rinci penggunaan teknologi AI dalam berbagai aspek kehidupan, Indonesia masih tertinggal dalam penanganan kejahatan digital berbasis AI. Negara-negara tersebut sudah memiliki kerangka hukum yang lebih adaptif, sementara Indonesia masih menghadapi kekosongan hukum yang menghambat penegakan hukum terhadap kejahatan berbasis teknologi AI.

Dalam analisis hukum atas tindak pidana penipuan melalui rekaman suara berbasis AI, secara normatif penipuan ialah tindakan memperdaya seseorang dengan tujuan meraih keuntungan yang melawan hukum dan mengakibatkan kerugian pihak lain. Rekaman suara AI dipahami sebagai alat baru untuk melakukan kriminalitas dengan meniru suara asli korban atau pihak lain secara meyakinkan, sehingga korban mudah terperdaya. Dalam praktik hukum, keabsahan rekaman suara sebagai barang bukti sangat penting, namun dengan kemunculan teknologi AI, hal ini menjadi rumit. Validitas rekaman hasil AI harus didukung oleh teknologi forensik yang mampu membedakan antara suara asli dan suara sintesis, tantangan yang hingga saat ini masih dalam proses perkembangan. Pertanggungjawaban pidana pelaku dalam kasus ini tidak hanya terbatas pada orang yang secara langsung melakukan penipuan, tetapi juga artis AI pembuat teknologi, operator, dan penyebar konten yang dengan sengaja memfasilitasi tindak pidana, sehingga perlu perluasan interpretasi hukum untuk mengakomodasi semua pihak yang terlibat.

Adapun regulasi di Indonesia yang relevan terdiri dari KUHP Pasal 378 sebagai dasar hukum umum penipuan, UU ITE yang mengatur kejahatan di bidang teknologi informasi, dan peraturan tambahan seperti UU Perlindungan Data Pribadi dan peraturan keamanan siber. Namun, ketiga instrumen ini belum secara khusus mengatur rekaman suara AI, sehingga efektivitas penindakan terhadap penipuan

deepfake masih terbatas. Kesulitan ini diperparah dengan kurangnya kemampuan teknis aparat penegak hukum dalam mengidentifikasi suara AI dan dalam proses pembuktian di pengadilan. Penegakan hukum saat ini masih dilakukan secara konvensional yang belum didukung penuh oleh teknologi dan pengetahuan yang memadai, menyebabkan rendahnya angka keberhasilan penindakan kasus semacam ini. Oleh karena itu, sinergi antara pengembangan kapasitas sumber daya manusia, legal drafting regulasi baru, dan pemanfaatan teknologi forensik mutakhir menjadi kebutuhan mendesak.

Di level internasional, prinsip hukum universal mengenai penipuan dan perlindungan data digital juga dapat dijadikan referensi, misalnya Konvensi Budapest tentang Kejahatan Dunia Maya dan aturan *European Union General Data Protection Regulation* (GDPR) yang memiliki persamaan asas dengan perlindungan individu dari penipuan AI di Indonesia.¹⁴ Dengan dasar-dasar hukum tersebut, penegakan hukum terhadap penipuan berbasis rekaman suara AI di Indonesia saat ini dijalankan melalui penafsiran norma secara progresif, mengingat regulasi spesifik tentang AI dan rekaman suara digital belum tersedia secara lengkap. Urgensi penguatan dan pembaruan regulasi menjadi kebutuhan mendesak, baik dengan revisi UU ITE maupun pengesahan peraturan pelaksana yang spesifik untuk pengaturan teknologi AI, deepfake voice, dan rekaman suara digital. Legal drafting yang komprehensif dan adaptif harus memperhatikan perkembangan teknologi, social engineering, dan perlindungan hukum bagi korban serta upaya mitigasi risiko kejahatan ekonomi digital secara berkelanjutan.

Keseluruhan permasalahan yang diuraikan menunjukkan bahwa tindak pidana penipuan berbasis rekaman suara AI merupakan bentuk kejahatan ekonomi yang memiliki dimensi filosofi, hukum, dan sosial yang kompleks. Tantangan besar hadir di tengah dinamika perkembangan teknologi yang cepat, sementara regulasi dan kesadaran sosial masih tertinggal. Kondisi ini memerlukan perhatian serius dari berbagai pemangku kepentingan untuk merancang strategi hukum yang adaptif, komprehensif, dan berkelanjutan guna melindungi masyarakat dan menjaga keadilan ekonomi dalam era digital.

¹⁴ Dhoni Martien, *Perlindungan Hukum Data Pribadi*, Mitra Ilmu, Makassar, 2023, p.68.

2. Upaya Penanganan atas Tindak Pidana Penipuan melalui Rekaman Suara Berbasis Kecerdasan Buatan (AI)

Dalam rangka menghadapi maraknya tindak pidana penipuan yang menggunakan rekaman suara berbasis kecerdasan buatan (AI), diperlukan langkah-langkah strategis, taktis, dan komprehensif yang melibatkan regulasi, teknologi, penegakan hukum, serta edukasi masyarakat. Upaya ini bersifat multidimensional dan harus berlangsung secara simultan agar mampu mengatasi kompleksitas masalah yang muncul akibat perkembangan teknologi deepfake voice.¹⁵

Pertama, penguatan regulasi merupakan fondasi utama dalam penanganan penipuan suara AI. Pemerintah telah menyiapkan kerangka dasar berupa UU ITE, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta revisi KUHP. Namun, pembaharuan khusus yang mengatur secara rinci teknologi AI deepfake dan implikasi pidananya harus segera diimplementasikan. Regulasi yang adaptif perlu mengakomodasi aspek otentikasi data suara digital, standar bukti elektronik, dan pengaturan tanggung jawab hukum pelaku. Pembuatan peta jalan nasional mengenai teknologi AI yang sedang dikembangkan oleh pemerintah Indonesia menjadi langkah progresif untuk memastikan teknologi ini digunakan secara positif dan risiko negatifnya tertangani dengan efektif.

Kedua, pengembangan dan penerapan teknologi deteksi serta mitigasi sangat penting dalam menekan ruang gerak penipu. Beberapa teknologi seperti *automatic speaker verification* (ASV), *deepfake detection algorithms*, dan termasuk teknologi interruptor suara seperti ASRJam yang mengganggu bot suara AI secara halus, menjadi alat vital membantu aparat dan instansi keamanan dalam mengidentifikasi rekaman palsu. Pendekatan ini perlu diintegrasikan dalam sistem keamanan perbankan, transaksi elektronik, dan layanan telekomunikasi untuk mencegah terjadinya transaksi penipuan secara real-time. Kolaborasi lembaga pemerintah, swasta, dan komunitas teknologi harus ditingkatkan untuk mengembangkan inovasi teknologi yang sesuai dengan karakter dan kebutuhan Indonesia.¹⁶

¹⁵ Budi Handoyo dkk., *Tinjauan Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008*, MAQASIDI: Jurnal Syariah Dan Hukum, Vol.4, No.1 (2024).

¹⁶ Deny Jollyta, Dwi Oktarina dan Johan Johan, *Tinjauan Kasus Model Speech Recognition: Hidden Markov Model*, Jurnal Edukasi Dan Penelitian Informatika (JEPIN), Vol.6, No.2 (2020), p.202.

Ketiga, peningkatan kapasitas sumber daya manusia di aparat penegak hukum dan lembaga pengawas menjadi faktor kunci keberhasilan penanganan kasus penipuan AI. Pelatihan tentang teknologi forensik digital, teknik investigasi siber, hingga pemahaman konsep dan modus operandi deepfake harus menjadi bagian dari pelatihan reguler bagi penegak hukum, jaksa, dan hakim.¹⁷ Hal ini akan memperkecil kesalahan dalam proses penyidikan dan persidangan, serta memperkuat bukti dan proses penuntutan.

Keempat, edukasi dan peningkatan literasi digital kepada masyarakat luas menjadi upaya preventif yang sangat penting. Kampanye edukasi tentang modus penipuan deepfake suara, cara mengenali ciri-cirinya, serta langkah tepat yang harus diambil jika menerima panggilan mencurigakan harus gencar dilakukan. Misalnya, masyarakat diimbau untuk tidak mudah terpengaruh oleh tekanan yang disampaikan lewat telepon dengan suara yang sangat meyakinkan, mencurigai panggilan mendesak yang meminta transfer uang, dan melakukan verifikasi ulang melalui saluran resmi keluarga atau lembaga terkait. Contoh konkret adalah meminta penelepon menjawab pertanyaan spesifik yang hanya diketahui korban dan penelepon asli. Pemerintah dan organisasi masyarakat sipil dapat bekerja sama untuk menyediakan materi edukasi berbasis media sosial, seminar-seminar, dan pelatihan teknis bagi kelompok rentan seperti lansia.¹⁸

Kelima, sistem pelaporan dan layanan pengaduan yang responsif dan mudah diakses wajib dikembangkan. Korban yang mengalami penipuan suara AI perlu mendapat pendampingan dan perlindungan hukum yang efektif. Layanan pengaduan digital yang terintegrasi dengan aparat kepolisian dan lembaga perlindungan konsumen akan mempercepat penanganan. Data dari pelaporan ini selanjutnya dapat dianalisis untuk mendeteksi pola modus dan memperbarui strategi pencegahan serta penanganan.¹⁹

¹⁷ Patricia Morisa Banfatin, Karolus Kopong Medan dan Debi F.Ng. Fallo, *Pengaturan Hukum Pidana di Indonesia terhadap Penyalahgunaan Teknologi Artificial Intelligence Deepfake dalam Melakukan Tindak Pidana Cybercrime*, Pemuliaan Keadilan, Vol.2, No.1 (2024), p.64.

¹⁸ Najwa Fathiro Cahyono, Khurrotul 'Uyun dan Siti Mukaromah, *Etika Penggunaan Kecerdasan Buatan pada Teknologi Informasi*, Prosiding Seminar Nasional Teknologi Dan Sistem Informasi, Vol.3, No.1 (2023).

¹⁹ Dikdik M. Arief Mansur dan Elisatris, *Cyber Law Aspek Hukum Teknologi Informasi*, PT Refika Aditama, Bandung, 2009.

Keenam, perbandingan dan belajar dari regulasi di negara lain juga menjadi hal yang penting. Negara-negara maju seperti Amerika Serikat, Inggris, dan Uni Eropa telah mengembangkan aturan dan pedoman khusus untuk menangani deepfake dan penipuan suara AI, termasuk pengenalan sanksi pidana baru yang tegas dan pembentukan lembaga khusus untuk menangani kasus kejahatan siber. Adaptasi kebijakan tersebut disesuaikan dengan hukum dan sosial Indonesia sehingga menghasilkan sistem hukum yang komprehensif dan efektif.²⁰

Dengan mengintegrasikan seluruh upaya ini secara terpadu, Indonesia dapat membangun sistem perlindungan hukum dan keamanan siber yang tangguh terhadap ancaman penipuan rekaman suara berbasis kecerdasan buatan. Hal ini akan memperkuat kepercayaan publik dalam penggunaan teknologi digital, sekaligus menjaga stabilitas ekonomi dan sosial di era transformasi digital yang terus berkembang.

C. PENUTUP

Kesimpulan dari penelitian ini menunjukkan bahwa penipuan berbasis rekaman suara yang dihasilkan oleh kecerdasan buatan (AI) semakin marak dan menjadi tantangan serius bagi sistem hukum Indonesia. Hukum yang ada saat ini, seperti KUHP dan UU ITE, belum mampu mengakomodasi perkembangan teknologi AI yang begitu pesat. Kekosongan hukum ini menciptakan celah yang memungkinkan pelaku kejahatan memanfaatkan teknologi ini tanpa adanya sanksi yang jelas. Oleh karena itu, pembaruan regulasi yang lebih responsif terhadap teknologi AI sangat diperlukan. Saran yang dapat diberikan adalah untuk segera merevisi regulasi yang ada dan menciptakan undang-undang yang lebih spesifik terkait penggunaan AI dalam kejahatan, serta meningkatkan kapasitas aparat penegak hukum dalam menangani kasus-kasus digital berbasis teknologi AI.

²⁰ Dikdik M. Arief Mansur dan Elisatris, *Cyber Law Aspek Hukum Teknologi Informasi*, PT Refika Aditama, Bandung, 2009.

DAFTAR PUSTAKA

Buku

- Elisatris, Dikdik M. Arief Mansur. 2009. *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: PT Refika Aditama.
- Martien, Dhoni. 2023. *Perlindungan Hukum Data Pribadi*. Makassar: Mitra Ilmu.
- Pusat Pendidikan dan Pelatihan. 2010 *Azaz-Azaz Hukum Pidana*. Jakarta: PPPJ.

Publikasi

- Handoyo, Budi, Husamuddin MZ, Ida Rahma dan Asy'ari. *Tinjauan Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008*. MAQASIDI. Vol.4. No.1 (2024).
- Haris, Muhammad Tan Abdul Rahman dan Tantimin. *Analysis of Criminal Law Liability for the Use of Artificial Intelligence in Indonesia*. Jurnal Komunikasi Hukum (JKH). Vol.8. No.1 (2022).
- Jollyta, Deny, Dwi Oktarina dan Johan Johan. *Tinjauan Kasus Model Speech Recognition: Hidden Markov Model*. Jurnal Edukasi Dan Penelitian Informatika (JEPIN). Vol.6. No.2 (2020).
- Najwa Fathiro Cahyono, Khurrotul 'Uyun dan Siti Mukaromah. *Etika Penggunaan Kecerdasan Buatan pada Teknologi Informasi*. Prosiding Seminar Nasional Teknologi Dan Sistem Informasi. Vol.3. No.1 (2023).
- Patricia Morisa Banfatin, Karolus Kopong Medan dan Debi F.Ng. Fallo. *Pengaturan Hukum Pidana di Indonesia terhadap Penyalahgunaan Teknologi Artificial Intelligence Deepfake dalam Melakukan Tindak Pidana Cybercrime*. Pemuliaan Keadilan. Vol.2. No.1 (2024).
- Peta, Saphalya. *Journey of Artificial Intelligence Frontier: A Comprehensive Overview*. Global Journal of Computer Science and Technology. Vol.23, Issue 2 (2023).
- Pusdiana, Made Sadika, Ediwarman Ediwarman, Sunarmi Sunarmi dan Mohammad Ekaputra. *Penegakan Hukum terhadap Tindak Pidana Penipuan dengan Modus Arisan Online pada Polres Nias*. Locus. Vol.2. No.11 (2023).
- Ramadhani, Fitria. *Kesenjangan Regulasi Kecerdasan Buatan di Indonesia: Analisis Komparatif dengan Artificial Intelligence Act Uni Eropa*. Legislasi Indonesia. Vol.20. No.1 (2022).
- Ririh, Kirana Rukmayuninda, Nur Laili, Adityo Wicaksono dan Silmi Tsurayya. *Studi Komparasi dan Analisis SWOT pada Implementasi Kecerdasan Buatan (Artificial Intelligence) di Indonesia*. Jurnal Teknik Industri. Vol.15. No.2 (2020).
- Surden, Harry. *Artificial Intelligence and Law: An Overview*. Georgia State University Law Review. Vol.35 (2019).
- Surya, Faizal Adi. *Perlindungan Hukum Korban Kekerasan Seksual dalam Pemberitaan Media Online di Indonesia*. Jurnal Hukum Samudra Keadilan. Vol.17. No.1 (2022).

Karya Ilmiah

- Afnan, Hafsha Amalia. 2022. *Perlindungan Hukum Penyalahgunaan Artificial Intelligence Deepfake pada Layanan Pinjaman Online*. Surakarta: Universitas Muhammadiyah Surakarta.

Website

Dwipratama, Gede Priana. *Implikasi Kecerdasan Buatan dalam Industri Pertahanan: Tantangan dan Peluang bagi Indonesia*. diakses dari <https://www.kemhan.go.id/poahan/2024/03/20/implikasi-kecerdasan-buatan-dalam-industri-pertahanan-tantangan-dan-peluang-bagi-indonesia.html>. diakses pada 18 Desember 2025.

Sumber Hukum

Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

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

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

