J-CEKI: Jurnal Cendekia Ilmiah
Vol.4, No.2, Februari 2025

Perkembangan *Artificial Intelligence* terhadap Tindak Pidana Penipuan di Indonesia

Undang Prasetya Umara[1], Haykal Faqih Aldika[2], Shofa Fathiyah[3], Imran Bukhari Razif[4]
[1,2,3,4]Universitas Muhammadiyah Tangerang, Indonesia
E-mail: undang.prasetya@umt.ac.ad[1]

Article History:
Received: 31 Januari 2025
Revised: 25 Februari 2025
Accepted: 28 Februari 2025

Keywords: *Artificial intelligence; deepfake; penipuan digital; kejahatan siber; penegakan hukum; hukum pidana digital*

Abstract: *Perkembangan Artificial Intelligence (AI) telah menghadirkan peluang baru dalam berbagai sektor, tetapi pada saat yang sama membuka ruang bagi munculnya bentuk kejahatan digital yang semakin kompleks, termasuk penipuan berbasis teknologi deepfake. Di Indonesia, kemunculan konten manipulatif yang menyerupai figur publik, termasuk kasus penipuan yang menggunakan citra Prabowo Subianto, menunjukkan bahwa kemajuan teknologi belum sepenuhnya diikuti oleh kesiapan sistem hukum dalam merespons bentuk kejahatan digital yang baru. Penelitian ini bertujuan menganalisis perkembangan penggunaan AI dalam tindak pidana penipuan di Indonesia, mengkaji konstruksi hukum yang dapat digunakan untuk menjerat pelaku, serta mengevaluasi praktik penegakan hukumnya. Penelitian ini menggunakan metode hukum normatif-empiris melalui kajian terhadap peraturan perundang-undangan, studi literatur, dan data empiris yang diperoleh melalui wawancara dengan aparat penegak hukum. Hasil penelitian menunjukkan bahwa Indonesia belum memiliki regulasi khusus yang secara eksplisit mengatur penyalahgunaan teknologi deepfake. Meskipun demikian, ketentuan dalam Undang-Undang Nomor 1 Tahun 2024 dan Kitab Undang-Undang Hukum Pidana masih dapat digunakan sebagai dasar penegakan hukum. Namun, implementasinya masih menghadapi kendala berupa kompleksitas teknologi, pembuktian digital, dan keterbatasan kapasitas teknis aparat. Penelitian ini menegaskan urgensi pembaruan regulasi dan penguatan kapasitas penegakan hukum guna menjamin kepastian hukum dan perlindungan masyarakat di era kejahatan berbasis AI.*

PENDAHULUAN

Perkembangan teknologi digital dalam beberapa dekade terakhir telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam bidang hukum dan kejahatan. Salah satu inovasi teknologi yang berkembang pesat adalah *Artificial Intelligence* (AI), yang memiliki kemampuan untuk meniru kecerdasan manusia dalam memproses data, mengambil keputusan, serta menghasilkan konten digital secara otomatis. Di satu sisi, AI memberikan manfaat besar dalam meningkatkan efisiensi dan produktivitas, namun di sisi lain juga membuka peluang baru

bagi munculnya kejahatan berbasis teknologi yang semakin kompleks dan sulit dideteksi.

Salah satu bentuk penyalahgunaan AI yang saat ini menjadi perhatian global adalah teknologi *deepfake*. Teknologi ini memungkinkan manipulasi wajah, suara, dan gerakan seseorang dalam bentuk video atau audio sehingga tampak sangat realistis dan sulit dibedakan dari konten asli. Perkembangan *deepfake* telah mendorong munculnya berbagai modus kejahatan baru, khususnya tindak pidana penipuan (*fraud*), yang memanfaatkan kepercayaan publik terhadap figur tertentu atau informasi visual yang tampak autentik.

Di Indonesia, fenomena penipuan berbasis *deepfake* mulai menunjukkan peningkatan yang signifikan. Kasus yang sempat menjadi perhatian publik adalah penggunaan video *deepfake* yang menampilkan sosok Presiden Prabowo Subianto untuk menawarkan bantuan sosial palsu kepada masyarakat. Namun demikian, kasus serupa tidak hanya terbatas pada figur pejabat negara. Modus penipuan juga berkembang dengan menggunakan wajah tokoh publik, selebritas, hingga pimpinan perusahaan untuk meyakinkan korban agar mentransfer sejumlah uang. Selain itu, terdapat pula kasus penipuan berbasis suara (*voice cloning*) yang meniru suara anggota keluarga atau pimpinan perusahaan untuk meminta transfer dana secara mendesak, serta penipuan investasi ilegal yang menggunakan video AI untuk menciptakan testimoni palsu dari figur terkenal.

Fenomena tersebut menunjukkan bahwa perkembangan AI telah menggeser pola kejahatan konvensional menjadi kejahatan digital yang lebih sistematis, masif, dan sulit dilacak. Hal ini menimbulkan tantangan serius dalam sistem hukum pidana Indonesia, baik dari aspek regulasi maupun penegakan hukum. Hingga saat ini, Indonesia belum memiliki pengaturan hukum yang secara khusus mengatur penyalahgunaan teknologi *deepfake*. Penegakan hukum masih bergantung pada ketentuan umum seperti Pasal 35 juncto Pasal 51 Undang-Undang Informasi dan Transaksi Elektronik serta Pasal 378 Kitab Undang-Undang Hukum Pidana tentang penipuan.

Beberapa penelitian sebelumnya menunjukkan bahwa kejahatan siber terus berkembang seiring kemajuan teknologi, dan regulasi yang ada seringkali tertinggal dibandingkan dengan inovasi teknologi (Rohmy et al., 2021). Penelitian lain juga menekankan bahwa *deepfake* berpotensi besar digunakan dalam penyebaran disinformasi, pencemaran nama baik, hingga penipuan digital yang merugikan masyarakat secara luas (Bonda Sisephaputra, 2024). Namun demikian, kajian yang secara spesifik mengkaji hubungan antara perkembangan AI, teknologi *deepfake*, dan tindak pidana penipuan dalam konteks hukum Indonesia masih terbatas.

Berdasarkan kondisi tersebut, penelitian ini menjadi penting untuk dilakukan guna mengkaji bagaimana perkembangan *Artificial Intelligence* mempengaruhi tindak pidana penipuan di Indonesia, serta bagaimana sistem hukum yang ada merespons fenomena tersebut. Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan ilmu hukum pidana, khususnya dalam menghadapi tantangan kejahatan berbasis teknologi, serta menjadi dasar rekomendasi bagi pembentukan regulasi yang lebih adaptif terhadap perkembangan teknologi digital.

LANDASAN TEORI

Perkembangan *Artificial Intelligence* (AI) merupakan bagian integral dari transformasi digital global yang secara signifikan mempengaruhi berbagai aspek kehidupan manusia, termasuk dalam bidang hukum. Secara konseptual, AI didefinisikan sebagai kemampuan sistem komputer untuk melakukan fungsi-fungsi yang umumnya membutuhkan kecerdasan manusia, seperti pembelajaran, penalaran, dan pengambilan keputusan. John McCarthy sebagai pelopor AI menyatakan bahwa AI adalah “ilmu dan rekayasa untuk membuat mesin cerdas” yang mampu meniru kecerdasan manusia. Definisi ini diperkuat oleh Stuart Russell dan Peter Norvig yang menyebutkan bahwa AI adalah studi tentang agen rasional yang bertindak untuk mencapai tujuan

tertentu berdasarkan persepsi terhadap lingkungannya.

Dalam konteks hukum, AI tidak hanya dipandang sebagai alat bantu, tetapi juga sebagai sarana potensial terjadinya kejahatan baru. Hal ini sejalan dengan pandangan Lawrence Lessig yang menyatakan bahwa "code is law", yaitu bahwa teknologi (kode) dapat membentuk perilaku manusia layaknya hukum itu sendiri. Dengan demikian, perkembangan AI dapat menciptakan norma sosial baru sekaligus membuka ruang bagi penyalahgunaan teknologi.

Salah satu bentuk konkret dari perkembangan AI adalah teknologi *deepfake*, yang memanfaatkan *deep learning* dan algoritma *Generative Adversarial Networks* (GAN). Menurut Ian Goodfellow, GAN bekerja melalui dua jaringan saraf yang saling berkompetisi untuk menghasilkan konten yang semakin realistis. Teknologi ini memungkinkan manipulasi wajah, suara, dan gerakan seseorang secara sangat meyakinkan. Chesney dan Danielle Citron menjelaskan bahwa *deepfake* merupakan ancaman serius karena dapat digunakan untuk menyebarkan disinformasi, merusak reputasi, serta melakukan penipuan dengan tingkat kredibilitas tinggi. Dalam perspektif teori manipulasi informasi, *deepfake* menciptakan apa yang disebut sebagai *fabricated reality*, yaitu realitas yang direkayasa sehingga sulit dibedakan dari kenyataan.

Dalam hukum pidana, tindak pidana penipuan secara klasik diatur dalam Pasal 378 KUHP. Menurut Moeljatno, penipuan merupakan perbuatan yang dilakukan dengan tipu muslihat atau rangkaian kebohongan untuk menggerakkan orang lain menyerahkan sesuatu demi keuntungan pelaku. Unsur utama dalam penipuan adalah adanya kehendak untuk menguntungkan diri sendiri secara melawan hukum melalui cara-cara yang menyesatkan. Pendapat ini sejalan dengan R. Soesilo yang menekankan bahwa penipuan selalu berkaitan dengan manipulasi kepercayaan korban.

Dalam perkembangan modern, konsep penipuan telah berevolusi menjadi *cyber fraud*, yaitu penipuan yang dilakukan melalui media elektronik. Menurut David S. Wall, kejahatan siber memiliki karakteristik utama berupa anonimitas, sifat lintas batas, dan ketergantungan pada teknologi. Hal ini menyebabkan kejahatan menjadi lebih sulit dideteksi dan ditangani. Dalam konteks AI, penipuan berbasis *deepfake* memperkuat unsur tipu muslihat karena pelaku dapat memanfaatkan visual dan audio yang tampak autentik, sehingga meningkatkan tingkat keberhasilan kejahatan.

Selanjutnya, untuk menganalisis efektivitas penegakan hukum terhadap fenomena ini, digunakan teori sistem hukum dari Lawrence M. Friedman yang menyatakan bahwa sistem hukum terdiri dari tiga unsur utama, yaitu struktur hukum, substansi hukum, dan budaya hukum. Struktur hukum mencakup lembaga penegak hukum, substansi hukum mencakup peraturan perundang-undangan, dan budaya hukum mencakup kesadaran masyarakat terhadap hukum. Friedman menegaskan bahwa ketiga unsur ini harus berjalan secara sinergis agar penegakan hukum dapat efektif. Dalam konteks kejahatan berbasis AI, kelemahan pada substansi hukum (belum adanya regulasi khusus) dan budaya hukum (rendahnya literasi digital) menjadi hambatan utama dalam penegakan hukum.

Selain itu, teori perlindungan hukum juga menjadi relevan dalam penelitian ini. Satjipto Rahardjo menyatakan bahwa hukum harus bersifat progresif dan mampu melindungi masyarakat dari perkembangan sosial yang dinamis. Hukum tidak boleh statis, melainkan harus adaptif terhadap perubahan, termasuk perkembangan teknologi. Sementara itu, teori kepastian hukum menekankan pentingnya aturan yang jelas dan tidak multitafsir. Menurut Gustav Radbruch, hukum harus memenuhi tiga nilai dasar, yaitu keadilan, kemanfaatan, dan kepastian hukum. Dalam konteks AI, belum adanya regulasi khusus mengenai *deepfake* menunjukkan adanya ketidakseimbangan antara ketiga nilai tersebut.

Dari perspektif kriminologi, perkembangan kejahatan berbasis AI dapat dijelaskan melalui teori *technological determinism*, yang menyatakan bahwa teknologi mempengaruhi perilaku manusia, termasuk dalam melakukan kejahatan. Hal ini diperkuat oleh teori *routine activity* dari Lawrence E. Cohen dan Marcus Felson yang menyebutkan bahwa kejahatan terjadi ketika terdapat tiga unsur, yaitu pelaku yang termotivasi, korban yang rentan, dan tidak adanya pengawasan yang efektif. Dalam kasus penipuan berbasis AI, pelaku memanfaatkan teknologi canggih, korban umumnya memiliki literasi digital yang rendah, dan sistem pengawasan belum mampu mengimbangi perkembangan teknologi.

Dengan demikian, berdasarkan berbagai teori dan pendapat ahli tersebut, dapat disimpulkan bahwa perkembangan *Artificial Intelligence*, khususnya teknologi *deepfake*, telah menciptakan paradigma baru dalam tindak pidana penipuan. Kejahatan tidak lagi bergantung pada interaksi fisik, melainkan pada manipulasi persepsi digital yang semakin sulit dideteksi. Oleh karena itu, diperlukan pendekatan hukum yang komprehensif, meliputi pembaruan regulasi, peningkatan kapasitas aparat penegak hukum, serta penguatan literasi digital masyarakat sebagai langkah preventif dalam menghadapi kejahatan berbasis teknologi.

METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian yuridis normatif, yaitu penelitian hukum yang dilakukan dengan cara menelaah bahan pustaka atau data sekunder sebagai sumber utama. Penelitian yuridis normatif bertujuan untuk mengkaji dan menganalisis norma hukum yang mengatur serta berkaitan dengan perkembangan *Artificial Intelligence* (AI) dalam tindak pidana penipuan di Indonesia, khususnya dalam konteks teknologi *deepfake*.

Pendekatan yang digunakan dalam penelitian ini meliputi beberapa pendekatan, yaitu pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai peraturan yang relevan, seperti Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Informasi dan Transaksi Elektronik, serta Undang-Undang Perlindungan Data Pribadi. Pendekatan konseptual digunakan untuk memahami konsep-konsep hukum terkait *Artificial Intelligence*, *deepfake*, dan *cybercrime* berdasarkan doktrin dan pendapat para ahli hukum. Sementara itu, pendekatan kasus digunakan untuk mengkaji fenomena penipuan berbasis AI yang terjadi di Indonesia sebagai bentuk penerapan norma hukum dalam praktik.

Sumber bahan hukum dalam penelitian ini terdiri dari bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang relevan dengan objek penelitian. Bahan hukum sekunder berupa literatur ilmiah seperti buku, jurnal, hasil penelitian terdahulu, serta pendapat para ahli hukum yang berkaitan dengan topik penelitian. Adapun bahan hukum tersier berupa kamus hukum, ensiklopedia, serta sumber lain yang mendukung pemahaman terhadap bahan hukum primer dan sekunder.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*), yaitu dengan mengkaji dan menelaah berbagai dokumen hukum dan literatur yang relevan dengan penelitian. Selanjutnya, bahan hukum yang telah dikumpulkan dianalisis secara sistematis untuk memperoleh pemahaman yang komprehensif mengenai permasalahan yang diteliti.

Teknik analisis bahan hukum dalam penelitian ini menggunakan metode analisis kualitatif dengan pendekatan deskriptif-analitis. Analisis dilakukan dengan cara menginterpretasikan dan mengkonstruksi norma hukum yang berlaku, kemudian mengaitkannya dengan perkembangan teknologi *Artificial Intelligence* dalam tindak pidana penipuan. Penarikan kesimpulan dilakukan dengan menggunakan metode berpikir deduktif, yaitu menarik kesimpulan dari hal-hal yang

bersifat umum (norma hukum) ke hal-hal yang bersifat khusus (kasus penipuan berbasis AI). Alur penelitian ini dapat digambarkan sebagai berikut:

Identifikasi Isu Hukum → Penelusuran Bahan Hukum → Klasifikasi dan Analisis Norma → Interpretasi Hukum → Penarikan Kesimpulan

Melalui metode yuridis normatif ini, penelitian diharapkan mampu memberikan analisis yang mendalam terhadap kecukupan dan relevansi pengaturan hukum yang ada dalam menghadapi perkembangan tindak pidana penipuan berbasis *Artificial Intelligence* di Indonesia.

HASIL DAN PEMBAHASAN

Perkembangan *Artificial Intelligence* (AI), khususnya teknologi *deepfake* dan *voice cloning*, telah mengubah karakteristik tindak pidana penipuan dari yang bersifat konvensional menjadi berbasis manipulasi realitas digital. Teknologi ini memungkinkan produksi konten audio-visual yang sangat realistis sehingga meningkatkan efektivitas penipuan melalui eksploitasi kepercayaan korban (Chesney & Citron, 2019).

Pengaturan Hukum terhadap Penipuan Berbasis Artificial Intelligence

Secara normatif, Indonesia belum memiliki regulasi khusus yang secara eksplisit mengatur penyalahgunaan AI dalam tindak pidana penipuan. Namun, ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 35 juncto Pasal 51, dapat digunakan untuk menjerat pelaku yang melakukan manipulasi informasi elektronik agar tampak autentik (Sari et al., 2022). Selain itu, Pasal 378 KUHP tetap relevan sebagai dasar hukum penipuan karena mengandung unsur tipu muslihat dan rangkaian kebohongan.

Menurut Moeljatno, inti dari tindak pidana penipuan terletak pada tindakan menggerakkan orang lain melalui cara-cara yang menyesatkan untuk memperoleh keuntungan (Moeljatno, 2008). Dalam konteks AI, *deepfake* dan *voice cloning* memperkuat unsur tipu daya tersebut karena mampu menciptakan ilusi kebenaran yang sulit diverifikasi oleh korban.

Namun demikian, belum adanya pengaturan khusus terkait AI menimbulkan *legal gap*. Hal ini sejalan dengan pandangan bahwa hukum sering tertinggal dari perkembangan teknologi, sehingga membutuhkan adaptasi regulatif yang lebih responsif (Rohmy et al., 2021).

Modus Penipuan Berbasis AI: Analisis Kasus Konkret

Perkembangan teknologi AI telah melahirkan berbagai modus penipuan baru yang dapat diidentifikasi melalui beberapa kasus nyata berikut:

1. Kasus *Deepfake* Investasi dengan Figur Publik (Indonesia)

Di Indonesia, beredar video *deepfake* yang menampilkan figur publik, seperti artis dan tokoh ekonomi, yang seolah-olah memberikan testimoni terhadap platform investasi tertentu. Video tersebut disebarkan melalui media sosial dan digunakan untuk menarik korban agar melakukan investasi. Kasus ini menunjukkan bagaimana pelaku memanfaatkan kredibilitas sosial (*social trust*) untuk memperkuat tipu muslihat.

Fenomena ini sesuai dengan temuan bahwa *deepfake* memiliki kemampuan tinggi dalam membentuk persepsi publik dan memanipulasi kepercayaan (Zahro et al., 2024). Chesney dan Citron juga menegaskan bahwa teknologi ini berbahaya karena mampu "mengaburkan batas antara kebenaran dan kebohongan" (Chesney & Citron, 2019).

2. Kasus *Voice Cloning* dalam Penipuan Bisnis (Internasional)

Salah satu kasus yang banyak dirujuk adalah penipuan terhadap sebuah perusahaan energi di Inggris pada tahun 2019. Pelaku menggunakan teknologi AI untuk meniru suara CEO perusahaan induk dan menginstruksikan transfer dana sebesar €220.000 kepada rekening tertentu.

Korban percaya karena suara tersebut terdengar identik dengan suara asli CEO (Europol, 2022).

Kasus ini menunjukkan bahwa AI tidak hanya memanipulasi visual, tetapi juga suara, sehingga memperluas spektrum penipuan digital. Menurut Wall, kejahatan siber berkembang dengan memanfaatkan teknologi untuk mengeksploitasi kepercayaan korban dalam lingkungan digital yang anonim (Wall, 2007).

3. Kasus *Deepfake* dalam Penipuan Donasi dan Bantuan Sosial

Selain investasi, teknologi *deepfake* juga digunakan dalam penipuan berkedok bantuan sosial atau donasi. Pelaku membuat video yang menampilkan tokoh agama atau tokoh masyarakat yang seolah-olah mengajak masyarakat untuk berdonasi atau mengikuti program bantuan tertentu. Korban yang terpengaruh kemudian mentransfer sejumlah uang.

Kasus ini menunjukkan bahwa AI tidak hanya memanfaatkan rasionalitas korban, tetapi juga aspek emosional dan psikologis. Dalam perspektif kriminologi, hal ini berkaitan dengan teori *routine activity*, di mana pelaku memanfaatkan kelemahan korban dan minimnya pengawasan (Cohen & Felson, 1979).

4. Kasus Identitas Digital Palsu (*Romance Scam* Berbasis AI)

Perkembangan AI juga memungkinkan pembuatan identitas digital palsu yang sangat realistis. Dalam beberapa kasus *romance scam*, pelaku menggunakan foto dan video hasil AI untuk membangun hubungan emosional dengan korban sebelum akhirnya melakukan penipuan finansial. Menurut penelitian Interpol, penggunaan AI dalam kejahatan semacam ini meningkatkan tingkat keberhasilan penipuan karena korban sulit membedakan identitas asli dan palsu (Interpol, 2023).

5. Penegakan Hukum: Tantangan dan Keterbatasan

Berdasarkan teori sistem hukum dari Friedman, efektivitas penegakan hukum ditentukan oleh tiga unsur utama, yaitu struktur, substansi, dan budaya hukum (Friedman, 1975).

a. Substansi hukum: belum adanya regulasi khusus mengenai AI menyebabkan ketergantungan pada norma umum, sehingga menimbulkan ketidakpastian hukum.
b. Struktur hukum: keterbatasan teknologi dan keahlian aparat dalam mendeteksi *deepfake* menjadi kendala utama dalam pembuktian.
c. Budaya hukum: rendahnya literasi digital masyarakat membuat korban mudah tertipu oleh konten manipulatif.

Menurut Rahardjo, hukum harus bersifat progresif dan mampu beradaptasi dengan perubahan sosial, termasuk perkembangan teknologi (Rahardjo, 2009). Namun, dalam konteks AI, hukum di Indonesia masih bersifat reaktif.

6. Analisis Kritis dan Implikasi Hukum

Berdasarkan temuan penelitian, penipuan berbasis AI dapat dikategorikan sebagai bentuk *high-tech fraud*, yaitu kejahatan yang mengandalkan manipulasi teknologi untuk menciptakan realitas semu. Kejahatan ini memiliki dampak yang lebih luas dibandingkan penipuan konvensional karena:

a. Menjangkau korban dalam skala besar melalui media digital;
b. Sulit dideteksi karena tingkat realisme yang tinggi;
c. Berpotensi merusak kepercayaan publik terhadap informasi digital.

Lessig menyatakan bahwa teknologi memiliki kekuatan normatif yang dapat membentuk perilaku manusia layaknya hukum (*code is law*) (Lessig, 2006). Oleh karena itu, penyalahgunaan AI harus direspon tidak hanya melalui hukum, tetapi juga melalui pengaturan teknologi.

Dari perspektif kepastian hukum, kondisi ini menunjukkan bahwa regulasi yang ada belum mampu memenuhi prinsip keadilan, kemanfaatan, dan kepastian hukum sebagaimana dikemukakan oleh Radbruch (Radbruch, 1946).

Secara keseluruhan, hasil penelitian menunjukkan bahwa perkembangan *Artificial Intelligence* telah menciptakan paradigma baru dalam tindak pidana penipuan. Kasus-kasus yang terjadi, baik di Indonesia maupun internasional, menunjukkan bahwa AI telah menjadi instrumen utama dalam melakukan kejahatan berbasis manipulasi digital. Oleh karena itu, diperlukan reformasi hukum yang komprehensif, peningkatan kapasitas aparat penegak hukum, serta penguatan literasi digital masyarakat untuk menghadapi tantangan kejahatan di era AI.

KESIMPULAN

Perkembangan *Artificial Intelligence* (AI), khususnya teknologi *deepfake* dan *voice cloning*, telah mengubah secara fundamental pola tindak pidana penipuan di Indonesia menjadi lebih kompleks, persuasif, dan sulit dideteksi. Modus kejahatan tidak lagi bergantung pada interaksi langsung, melainkan pada manipulasi realitas digital yang mampu mengeksploitasi kepercayaan dan kelemahan literasi masyarakat.

Secara normatif, meskipun ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik serta Kitab Undang-Undang Hukum Pidana masih dapat digunakan untuk menjerat pelaku, namun belum terdapat pengaturan khusus yang secara komprehensif mengakomodasi karakteristik kejahatan berbasis AI. Hal ini menimbulkan kesenjangan hukum dan berimplikasi pada terbatasnya efektivitas penegakan hukum.

Oleh karena itu, diperlukan langkah strategis berupa pembaruan regulasi yang adaptif terhadap perkembangan teknologi, peningkatan kapasitas aparat penegak hukum dalam bidang digital forensik, serta penguatan literasi digital masyarakat sebagai upaya preventif. Pendekatan yang terintegrasi antara aspek hukum, teknologi, dan edukasi menjadi kunci dalam menghadapi tantangan tindak pidana penipuan di era *Artificial Intelligence*.

DAFTAR REFERENSI

Chesney, R., & Citron, Danielle Keats. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, *107*(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J

Citron, Danielle Keats. (2019). Sexual privacy. Yale Law Journal, *128*(7), 1870–1960.

Cohen, L. E., & Felson, Marcus. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, *44*(4), 588–608. https://doi.org/10.2307/2094589

Europol. (2022). *Facing reality? Law enforcement and the challenge of deepfakes*. The Hague: Europol.

Friedman, Lawrence M.. (1975). *The legal system: A social science perspective*. New York, NY: Russell Sage Foundation.

Interpol. (2023). *Global crime trend report 2023: Cyber-enabled fraud and AI threats*. Lyon: Interpol.

Lessig, Lawrence. (2006). *Code: Version 2.0*. New York, NY: Basic Books.

Moeljatno. (2008). *Asas-asas hukum pidana*. Jakarta: Rineka Cipta.

Radbruch, Gustav. (1946). Five minutes of legal philosophy. Oxford Journal of Legal Studies, *26*(1), 13–15. https://doi.org/10.1093/ojls/gqi042

Rahardjo, Satjipto. (2009). *Hukum progresif: Sebuah sintesa hukum Indonesia*. Yogyakarta: Genta Publishing.

Rohmy, A. M., Santoso, B., & Wibowo, A. (2021). Problematika hukum dalam penanggulangan cybercrime di Indonesia. Jurnal Hukum Ius Quia Iustum, *28*(1), 45–60.

https://doi.org/10.20885/iustum.vol28.iss1.art3

Sari, D. P., Nugroho, R., & Hidayat, T. (2022). Analisis yuridis manipulasi informasi elektronik dalam Undang-Undang ITE. Jurnal RechtsVinding, *11*(2), 233–245. https://doi.org/10.33331/rechtsvinding.v11i2.892

Wall, David S.. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity Press.

Zahro, F., Pratama, A., & Lestari, D. (2024). Deepfake sebagai ancaman disinformasi dan penipuan digital di era artificial intelligence. Jurnal Teknologi Informasi dan Hukum, *5*(1), 12–25.

Sisephaputra, A. B. (2024). Tantangan regulasi kecerdasan buatan dalam sistem hukum Indonesia. Jurnal Hukum dan Teknologi, *3*(2), 101–115.

Undang-Undang Nomor 1 Tahun 2024. (2024). *Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1*.

Undang-Undang Nomor 1 Tahun 2023. (2023). *Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842*.

Undang-Undang Nomor 27 Tahun 2022. (2022). *Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820*.