



URGENSI PEMBENTUKAN REGULASI ARTIFICIAL INTELLIGENCE DI INDONESIA DALAM PERSPEKTIF NEGARA HUKUM:

Studi Kasus Pemalsuan Identitas untuk Pembukaan Rekening Perbankan Berbasis AI

Alexsanro Gabe Simbolon*

Program Studi Hukum, Fakultas Hukum,
Universitas Pembangunan Nasional “Veteran” Jakarta
*Email corresponding author: 2310611275@mahasiswa.upnvj.ac.id

Abstract

The development of Artificial Intelligence (AI) in Indonesia, particularly in the banking sector, has increased the risk of identity fraud through deepfake technology in the electronic Know Your Customer (e-KYC) process. This study aims to analyze Indonesia's legal response to AI misuse and propose a regulatory model consistent with the rule of law. The research employs a normative legal method supported by conceptual and comparative approaches. The findings indicate that existing regulations have not provided legal certainty regarding liability for the misuse of generative AI. Therefore, risk-based legislation is needed to ensure legal certainty and public protection.

Keyword: Artificial Intelligence; Rule of Law; Identity Fraud; Regulation; Banking.

Abstrak

Perkembangan Artificial Intelligence (AI) di Indonesia, khususnya di sektor perbankan, meningkatkan risiko penyalahgunaan melalui pemalsuan identitas berbasis deepfake pada proses electronic Know Your Customer (e-KYC). Penelitian ini bertujuan menganalisis respons hukum positif Indonesia terhadap penyalahgunaan AI serta merumuskan model regulasi yang sesuai dengan prinsip negara hukum. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan konseptual dan perbandingan hukum. Hasil penelitian menunjukkan bahwa regulasi yang ada belum memberikan kepastian mengenai tanggung jawab atas penyalahgunaan AI generatif. Oleh karena itu, diperlukan regulasi berbasis risiko dalam bentuk undang-undang untuk menjamin kepastian hukum dan perlindungan masyarakat.

Kata Kunci: Artificial Intelligence; Negara Hukum; Pemalsuan Identitas; Regulasi; Perbankan.

1. PENDAHULUAN

Indonesia mengalami akselerasi adopsi teknologi kecerdasan artifisial yang signifikan dalam beberapa tahun terakhir. Pemerintah melalui Kementerian Komunikasi dan Digital mencatat tingkat pemanfaatan AI untuk produktivitas nasional yang tinggi, dan saat ini sedang menyiapkan dua rancangan Peraturan Presiden, yaitu mengenai peta jalan pengembangan AI dan etika tata kelola AI, yang ditargetkan terbit pada tahun 2026. Fakta ini menunjukkan bahwa negara menyadari urgensi tata kelola AI, namun pilihan instrumen hukum yang digunakan—Peraturan Presiden—patut dipertanyakan kecukupannya dari perspektif negara hukum, sebagaimana akan diuraikan lebih jauh pada bagian pembahasan.

Salah satu titik rawan penyalahgunaan AI yang paling konkret dan telah terjadi di lapangan adalah pemanfaatan teknologi deepfake, face-swapping, dan sintesis suara untuk mengelabui sistem electronic Know Your Customer (e-KYC) pada layanan pembukaan rekening bank digital. Modus ini memanfaatkan kelemahan verifikasi biometrik berbasis liveness detection yang sebagian masih dapat ditembus oleh wajah sintesis hasil generative AI, sehingga pelaku dapat membuka rekening atas nama orang lain tanpa kehadiran fisik maupun kesadaran pemilik identitas asli.¹

Rekening hasil pemalsuan tersebut kemudian lazim digunakan sebagai rekening penampung (rekening bodong) dalam tindak pidana lanjutan, seperti penipuan daring dan pencucian uang.

Penting untuk digarisbawahi sejak awal—dan ini adalah titik kritis yang sengaja ditonjolkan agar argumentasi artikel ini tidak jatuh pada simplifikasi—bahwa pemalsuan identitas itu sendiri bukan perbuatan baru yang lahir dari AI. Pemalsuan surat, pemalsuan identitas, dan penipuan telah diatur sejak lama dalam Kitab Undang-Undang Hukum Pidana (KUHP). Yang baru dan secara genuin memerlukan respons hukum bukanlah perbuatan pemalsuannya, melainkan tiga hal spesifik yang lahir dari karakteristik AI generatif: (1) skala produksi alat pemalsuan yang dapat dilakukan secara otomatis dan masif oleh satu pelaku tanpa keahlian teknis tinggi; (2) kesulitan pembuktian forensik digital untuk membedakan rekaman biometrik asli dan sintesis; dan (3) ambiguitas pertanggungjawaban ketika sistem AI milik bank sendiri—bukan milik pelaku—yang gagal mendeteksi pemalsuan tersebut akibat kelemahan algoritmis yang tidak dapat diprediksi sepenuhnya oleh perancangnya.²

Jika argumentasi “urgensi regulasi AI” dibangun tanpa memisahkan ketiga titik baru ini dari pemalsuan identitas konvensional, maka kesimpulannya akan terlalu mudah dan rentan dibantah, yakni seolah-olah cukup mengandalkan KUHP karena perbuatan dasarnya sama. Artikel ini akan menempatkan ketiga titik tersebut sebagai inti argumen mengapa regulasi khusus tetap diperlukan, bukan sekadar pengulangan retorika umum bahwa “teknologi baru memerlukan hukum baru”.

¹Gunawan, I. J., & Janisriwati, S. (2023). Legal Analysis on the Use of Deepfake Technology: Threats to Indonesian Banking Institutions. *Law and Justice*, 8(2), 192–210.

²Judijanto, L., Utama, A. S., & Setiyawan, H. (2025). Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia. *The Easta Journal Law and Human Rights*, 3(02), 101–109.

Dari sisi teori negara hukum, persoalan ini relevan karena tiga alasan. Pertama, asas kepastian hukum (*rechtszekerheid*) menuntut agar subjek hukum dapat mengetahui secara jelas norma yang mengatur perbuatannya, sementara saat ini terdapat kekaburan mengenai apakah penyelenggara jasa keuangan dapat dimintai pertanggungjawaban administratif maupun pidana atas kegagalan sistem AI yang dioperasikannya.³

Kedua, asas pembatasan kekuasaan (*limitation of power*) relevan ketika regulasi AI dirancang dalam bentuk Peraturan Presiden yang minim keterlibatan DPR, sehingga berpotensi mengurangi legitimasi demokratis dan akuntabilitas publik atas norma yang akan mengikat warga negara serta korporasi. Ketiga, asas perlindungan hak asasi manusia menuntut agar korban pemalsuan identitas berbasis AI memperoleh pemulihan (*remedy*) yang jelas, bukan terjebak dalam kekosongan forum akibat tumpang tindihnya kewenangan antara OJK, Kementerian Komdigi, dan aparat penegak hukum.

Artikel ini bermaksud menjawab pertanyaan: *pertama*, bagaimana pengaturan hukum terhadap penyalahgunaan Artificial Intelligence dalam kasus pemalsuan identitas untuk pembukaan rekening perbankan di Indonesia? *Kedua*, bagaimana model regulasi Artificial Intelligence yang sesuai dengan prinsip negara hukum di Indonesia?

2. METODE

Artikel ini disusun dengan metode penelitian hukum normatif (*doctrinal legal research*), yang menempatkan bahan hukum primer—peraturan perundang-undangan—sebagai objek kajian utama, ditunjang pendekatan konseptual (*conceptual approach*) untuk membongkar konsep negara hukum dan asas-asasnya, serta pendekatan perbandingan (*comparative approach*) terhadap kerangka regulasi AI di Uni Eropa (EU AI Act) sebagai pembanding model regulasi berbasis risiko. Bahan hukum sekunder berupa literatur akademik, pemberitaan resmi pemerintah, dan dokumen kebijakan digunakan untuk memetakan perkembangan rancangan regulasi AI nasional yang masih bersifat dinamis hingga pertengahan tahun 2026.

3. HASIL DAN PEMBAHASAN

3.1 Pengaturan Hukum terhadap Penyalahgunaan AI dalam Pemalsuan Identitas untuk Pembukaan Rekening Perbankan

Secara doktrinal, perbuatan memalsukan identitas seseorang untuk membuka rekening bank, terlepas dari sarana yang digunakan, telah dapat dijerat melalui sejumlah instrumen hukum pidana konvensional. Pasal 263 dan Pasal 266 KUHP (serta pasal terkait dalam UU No. 1 Tahun 2023 tentang KUHP Baru yang berlaku efektif tahun 2026) mengatur pemalsuan surat dan penggunaan keterangan palsu dalam akta autentik maupun di bawah tangan.⁴

³Rama, B. G. A., Prasada, D. K., & Mahadewi, K. J. (2023). Urgensi Pengaturan Artificial Intelligence (AI) dalam Bidang Hukum Hak Cipta di Indonesia. *Jurnal Rechtsens*, 12(2), 209–224.

⁴Pasal 263 dan Pasal 266 Kitab Undang-Undang Hukum Pidana (KUHP); lihat juga ketentuan terkait dalam Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Pasal 35 dan Pasal 51 UU No. 19 Tahun 2016 tentang Perubahan UU ITE mengatur secara spesifik larangan manipulasi, penciptaan, atau pengubahan informasi elektronik dengan tujuan agar informasi tersebut dianggap seolah-olah data otentik (pemalsuan dokumen elektronik).⁵

Ketentuan ini secara konseptual mampu menjangkau wajah sintetis atau suara hasil deepfake sepanjang dapat dibuktikan sebagai “informasi elektronik” yang dipalsukan.⁶

Meski demikian, konstruksi “informasi elektronik” dalam UU ITE pada dasarnya dirancang untuk menjangkau dokumen dan data digital secara umum, bukan secara spesifik untuk produk generative AI yang menghasilkan representasi biometrik sintetis (wajah, suara, maupun gerak) yang secara visual maupun audial nyaris tidak dapat dibedakan dari aslinya. Akibatnya, unsur “memanipulasi” atau “menciptakan seolah-olah otentik” dalam Pasal 35 UU ITE harus dimaknai secara ekstensif oleh aparat penegak hukum dan hakim melalui interpretasi kasus per kasus, yang pada gilirannya menciptakan ketidakseragaman penerapan hukum (inconsistency in legal application) antara satu perkara dengan perkara lain. Hal ini bertentangan dengan asas kepastian hukum yang menjadi salah satu pilar negara hukum, karena pelaku usaha maupun calon pelaku tindak pidana tidak memiliki kepastian mengenai batas perbuatan yang dilarang.

Di sisi sektor jasa keuangan, Otoritas Jasa Keuangan telah menerbitkan ketentuan teknis mengenai penerapan program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU-PPT) serta kewajiban prinsip mengenal nasabah (Customer Due Diligence) bagi bank yang menyelenggarakan layanan pembukaan rekening secara elektronik, termasuk persyaratan minimal terkait teknologi verifikasi wajah (face recognition) dan liveness detection.

UU No. 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK) memberikan dasar bagi OJK untuk mengatur lebih lanjut aspek teknologi dalam layanan keuangan digital, termasuk potensi pengenaan sanksi administratif terhadap bank yang lalai menerapkan standar keamanan.⁷

Namun demikian, ketentuan APU-PPT dan CDD tersebut pada dasarnya bersifat preventif-administratif dan ditujukan untuk mengatur hubungan bank dengan nasabah, bukan untuk mengatasi situasi ketika sistem AI itu sendiri yang menjadi titik kegagalan. Dengan kata lain, rezim pengawasan OJK saat ini lebih berorientasi pada kepatuhan prosedural (procedural compliance) ketimbang pada pengujian ketahanan teknis sistem AI terhadap serangan adversarial seperti deepfake, sehingga bank dapat secara formal dinyatakan “telah menerapkan CDD sesuai POJK” meskipun sistem AI yang digunakannya secara teknis rentan ditembus oleh wajah sintetis generasi terbaru.

Persoalannya bukan pada ketiadaan norma yang dapat menjerat pelaku individual, melainkan pada tiga gap normatif yang konkret.

Pertama, gap pembuktian. Hukum acara pidana Indonesia belum memiliki standar baku mengenai metode forensik digital untuk membuktikan keaslian rekaman biometrik di

⁵Pasal 35 dan Pasal 51 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

⁶Arvitto, R. S. (2025). Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP. *Jurnal Ilmiah Hukum dan Hak Asasi Manusia*, 4(2), 73–82.

⁷Undang-Undang Republik Indonesia Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan.

pengadilan, sehingga keterangan ahli mengenai keaslian wajah atau suara berisiko menjadi area abu-abu yang membuka ruang sengketa pembuktian berkepanjangan.⁸

Studi forensik digital pada konteks ujaran kebencian di media sosial menunjukkan bahwa metodologi penanganan barang bukti elektronik di Indonesia masih bertumpu pada kerangka umum hukum acara pidana yang dirancang untuk dokumen statis, bukan untuk konten yang dihasilkan secara dinamis oleh model generative AI. Tantangan ini menjadi lebih akut pada kasus deepfake biometrik dibandingkan ujaran kebencian tekstual, karena verifikasi keaslian wajah atau suara memerlukan keahlian khusus di bidang digital forensic image/audio analysis yang belum tersertifikasi secara baku oleh lembaga peradilan maupun kepolisian Indonesia. Tanpa standar baku ini, hakim pada akhirnya bergantung pada keterangan ahli yang metodenya dapat berbeda antara satu laboratorium forensik dengan laboratorium lainnya, sehingga membuka ruang bagi terdakwa untuk mengajukan ahli tandingan (counter expert) yang dapat memperlambat proses peradilan dan menimbulkan ketidakpastian hasil pemeriksaan.

Kedua, gap pertanggungjawaban korporasi. Ketika sistem AI milik bank gagal mendeteksi wajah sintetis akibat false negative pada model machine learning, belum terdapat norma yang secara tegas membedakan antara kelalaian operasional biasa (yang dapat dikenai sanksi administratif POJK) dan kegagalan struktural sistem AI yang disebabkan oleh desain algoritma itu sendiri (algorithmic failure), yang semestinya memunculkan tanggung jawab yang berbeda, termasuk kemungkinan tanggung jawab pengembang teknologi pihak ketiga (vendor AI) yang selama ini tidak diatur sebagai subjek hukum langsung dalam rezim perbankan.

Kekosongan ini menjadi semakin krusial mengingat sebagian besar bank di Indonesia tidak mengembangkan sistem face recognition dan liveness detection secara in-house, melainkan mengadakannya dari vendor teknologi pihak ketiga melalui mekanisme procurement dan lisensi perangkat lunak. Dalam hubungan hukum tersebut, perjanjian antara bank dan vendor pada umumnya mengatur pembagian risiko secara kontraktual (business-to-business liability allocation), yang sifatnya privat dan tidak otomatis mengikat atau melindungi nasabah selaku pihak ketiga yang dirugikan (third-party victim). Akibatnya, ketika terjadi kegagalan deteksi, korban—yaitu pemilik identitas asli yang disalahgunakan—berpotensi terjebak dalam proses pembuktian mengenai siapa yang sesungguhnya lalai: apakah bank yang kurang melakukan due diligence dalam memilih vendor, ataukah vendor yang model algoritmanya memang memiliki tingkat false negative tertentu yang secara teknis tidak dapat dihindari (inherent model limitation). Tanpa norma hukum publik yang secara eksplisit membebaskan tanggung jawab kepada salah satu atau kedua pihak demi melindungi korban, prinsip kepastian hukum dan perlindungan HAM dalam negara hukum tidak terpenuhi secara substantif.

Ketiga, gap kelembagaan. Kewenangan pengawasan tersebar antara OJK (aspek prudensial perbankan), Kementerian Komdigi (aspek tata kelola AI dan PSE), serta Kepolisian/Kejaksaan (aspek pidana), tanpa mekanisme koordinasi yang dibakukan dalam undang-undang, sehingga korban berpotensi menghadapi forum shopping yang membingungkan dan lambat.

Fragmentasi kelembagaan ini memunculkan dua risiko praktis. Di satu sisi, korban yang melapor ke kepolisian akan diproses melalui jalur pidana konvensional yang berfokus pada pembuktian unsur kesalahan pelaku individual, tanpa kewenangan untuk memerintahkan audit

⁸Medeline, F., Rusmiati, E., & Ramadhani, R. H. (2022). Forensik Digital dalam Pembuktian Tindak Pidana Ujaran Kebencian di Media Sosial. *PAMPAS: Journal of Criminal Law*, 3(3), 310–325.

teknis terhadap sistem AI bank. Di sisi lain, OJK sebagai otoritas pengawas perbankan memiliki kewenangan untuk memeriksa kepatuhan bank terhadap POJK, tetapi tidak memiliki yurisdiksi pidana untuk menindak pelaku pemalsuan maupun kewenangan teknis untuk menilai kelayakan algoritma AI yang digunakan, yang secara substansi lebih dekat dengan kompetensi Kementerian Komdigi. Tanpa adanya single point of coordination yang dibakukan dalam undang-undang, korban berisiko “dilempar” dari satu otoritas ke otoritas lain, dan proses pemulihan kerugian (restitusi maupun ganti rugi) menjadi berlarut-larut karena masing-masing lembaga hanya dapat menjangkau sebagian dari keseluruhan rantai peristiwa hukum.

Dengan demikian, jawaban atas rumusan masalah pertama adalah: pengaturan hukum yang ada saat ini bersifat memadai secara represif terhadap pelaku individual pemalsuan identitas, tetapi tidak memadai secara preventif dan struktural untuk mengatur risiko yang melekat pada teknologi AI itu sendiri, baik dalam aspek pembuktian, distribusi tanggung jawab korporasi-vendor, maupun koordinasi kelembagaan.

3.2 Model Regulasi AI yang Sesuai dengan Prinsip Negara Hukum di Indonesia

Konsep negara hukum (*rechtsstaat*) sebagaimana ditegaskan dalam Pasal 1 ayat (3) UUD NRI 1945 memuat sejumlah elemen pokok yang relevan dijadikan parameter dalam merancang regulasi AI, yaitu: (a) asas legalitas, di mana setiap pembatasan hak warga negara dan pembebanan kewajiban kepada pelaku usaha harus berdasar pada undang-undang, bukan semata produk hukum di bawahnya; (b) asas pembagian kekuasaan dan *check and balances*, yang menuntut keterlibatan lembaga legislatif dalam menetapkan norma yang berdampak luas; (c) asas perlindungan HAM, termasuk hak atas pemulihan bagi korban; dan (d) asas kepastian hukum serta non-diskriminasi dalam penerapan norma.⁹

Penekanan keempat asas tersebut sejalan dengan kajian mengenai urgensi pengaturan AI yang menempatkan kepastian hukum sebagai prasyarat utama tata kelola teknologi baru di Indonesia.¹⁰

Pilihan pemerintah untuk menuangkan tata kelola AI ke dalam Rancangan Peraturan Presiden tentang Peta Jalan AI dan Rancangan Peraturan Presiden tentang Etika AI patut dikritisi dari sudut pandang ini.¹¹

Secara hierarki norma berdasarkan UU No. 13 Tahun 2022 tentang Perubahan Kedua UU Pembentukan Peraturan Perundang-undangan, Peraturan Presiden berada di bawah undang-undang dan tidak dapat menciptakan delik pidana baru maupun membebaskan sanksi administratif yang signifikan tanpa dasar undang-undang yang jelas (asas legalitas dalam arti formil). Jika kewajiban substantif bagi penyelenggara sistem AI—termasuk klasifikasi risiko, audit algoritma, dan kewajiban pelaporan insiden—hanya diatur dalam Perpres, maka secara konstitusional daya ikat dan daya paksa terhadap korporasi maupun individu menjadi

⁹Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

¹⁰Rasyidah, N. A., Aksay, M., & Akmal, M. F. (2024). Urgensi Pembuatan Regulasi Penggunaan AI (Artificial Intelligence) Di Indonesia. *Jurnal Penegakan Hukum Indonesia*, 5(1), 42–51.

¹¹Lihat hierarki dan kedudukan Peraturan Presiden dalam Pasal 7 Undang-Undang Republik Indonesia Nomor 13 Tahun 2022 tentang Perubahan Kedua atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan.

lemah, dan rawan digugat melalui mekanisme judicial review ke Mahkamah Agung jika dianggap melampaui kewenangan delegasi.

Kekhawatiran sejumlah kalangan masyarakat sipil bahwa proses penyusunan Perpres AI berlangsung tertutup dan didorong oleh kepentingan bisnis serta politik elektoral, sebagaimana muncul dalam diskursus publik pada awal tahun 2026, juga memperkuat argumen bahwa proses legislasi yang lebih partisipatif melalui undang-undang—dengan pembahasan di DPR—lebih sesuai dengan asas pembagian kekuasaan dan akuntabilitas demokratis. Dalam perspektif teori negara hukum modern, partisipasi publik bukan sekadar formalitas prosedural, melainkan syarat legitimasi substantif (substantive legitimacy) dari norma yang akan membatasi hak warga negara maupun membebani pelaku usaha, terutama ketika norma tersebut menyangkut teknologi yang risikonya bersifat sistemik dan lintas sektor seperti AI.

Persoalan ini menjadi semakin relevan ketika dikaitkan dengan kasus deepfake yang telah benar-benar terjadi dan menimbulkan kerugian publik, sebagaimana terlihat pada modus penipuan deepfake yang mencatut figur publik untuk menawarkan bantuan uang palsu kepada masyarakat.¹²

Kasus tersebut, meskipun terjadi pada konteks penipuan publik secara umum dan bukan secara spesifik pada pembukaan rekening perbankan, memperlihatkan pola yang sama dengan yang dibahas dalam artikel ini: pelaku memanfaatkan kemudahan akses teknologi deepfake generatif untuk menciptakan kepercayaan palsu (false trust) pada korban, dan penanganannya pada akhirnya kembali bergantung pada delik pidana konvensional (penipuan, pencemaran nama baik, atau pelanggaran UU ITE) karena tidak adanya delik khusus yang menjangkau penyalahgunaan AI generatif itu sendiri. Hal ini menjadi indikasi empiris bahwa kekosongan regulasi yang diidentifikasi dalam pembahasan pertama bukan persoalan hipotetis, melainkan persoalan yang berulang pada berbagai sektor—baik perbankan maupun ranah sosial-politik—dan karenanya layak direspons dengan kerangka hukum yang bersifat lintas sektor (cross-sectoral), bukan hanya tambal sulam pada masing-masing undang-undang sektoral.

Sebagai pembandingan, Uni Eropa melalui Artificial Intelligence Act mengadopsi pendekatan regulasi berjenjang berbasis tingkat risiko (risk-based approach), yang mengklasifikasikan sistem AI ke dalam empat kategori: dilarang (unacceptable risk), risiko tinggi (high risk), risiko terbatas (limited risk), dan risiko minimal (minimal risk).¹³

Sistem AI yang digunakan untuk verifikasi identitas biometrik dalam layanan keuangan secara umum dikategorikan sebagai sistem berisiko tinggi yang dikenai kewajiban audit, transparansi algoritma, manajemen risiko berkelanjutan, dan kewajiban pelaporan insiden kepada otoritas pengawas, dengan sanksi administratif yang dapat dijatuhkan langsung berdasarkan undang-undang (regulation) yang mengikat seluruh negara anggota tanpa memerlukan instrumen hukum tambahan di tingkat nasional.

¹²Kristiyenda, Y. S., Faradila, J., & Basanova, C. (2025). Pencegahan Kejahatan Deepfake: Studi Kasus Terhadap Modus Penipuan Deepfake Prabowo Subianto Dalam Tawaran Bantuan Uang. ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora, 3(2), 149–164.

¹³Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), khususnya Pasal 5–6 mengenai klasifikasi tingkat risiko sistem AI.

Pendekatan berjenjang ini relevan untuk diadaptasi di Indonesia karena dua alasan. Pertama, secara filosofis pendekatan ini konsisten dengan asas proporsionalitas yang juga dikenal dalam tradisi negara hukum Indonesia, yaitu bahwa intensitas pengaturan dan pengawasan harus sebanding dengan besarnya risiko yang ditimbulkan suatu kegiatan, sehingga tidak semua sistem AI perlu diatur dengan tingkat kewajiban yang sama beratnya. Kedua, secara praktis pendekatan berjenjang memungkinkan regulator memprioritaskan sumber daya pengawasan pada sistem-sistem yang risikonya paling tinggi terhadap hak asasi dan kepentingan publik—seperti sistem verifikasi biometrik perbankan yang menjadi fokus artikel ini—tanpa harus membebani seluruh ekosistem inovasi AI nasional dengan kewajiban yang seragam dan kaku, yang berpotensi menghambat pertumbuhan industri teknologi domestik.

Berdasarkan perbandingan tersebut, model regulasi AI yang lebih sesuai dengan prinsip negara hukum di Indonesia idealnya memuat empat unsur berikut, yang masing-masing merespons langsung gap normatif yang telah diidentifikasi pada bagian pembahasan pertama:

- Dasar hukum setingkat undang-undang untuk norma inti (core obligations): klasifikasi risiko sistem AI, kewajiban audit algoritma bagi sistem berisiko tinggi (termasuk sistem verifikasi biometrik perbankan), dan ketentuan sanksi administratif maupun pidana, sehingga memenuhi asas legalitas formil dan melibatkan DPR sebagai representasi rakyat. Peraturan Presiden dan Peraturan Menteri dapat tetap digunakan, namun terbatas sebagai aturan pelaksana teknis, bukan sumber kewajiban substantif yang membatasi hak dan membebani sanksi. Unsur ini secara langsung merespons gap kelembagaan dan problem legitimasi yang melekat pada rencana regulasi berbentuk Perpres.
- Klasifikasi tegas sistem AI berisiko tinggi di sektor keuangan, termasuk sistem e-KYC, liveness detection, dan deteksi anti-fraud, dengan kewajiban audit independen secara periodik serta kewajiban pelaporan insiden kegagalan sistem (algorithmic incident reporting) kepada OJK dan Kementerian Komdigi secara terkoordinasi melalui satu pintu (single reporting gateway), guna menutup gap kelembagaan yang telah diuraikan pada bagian sebelumnya.
- Pembagian tanggung jawab yang eksplisit antara penyelenggara jasa keuangan (sebagai pengendali sistem/risk owner) dan pengembang teknologi AI pihak ketiga (sebagai penyedia komponen/technology provider), mengikuti model pertanggungjawaban berjenjang yang lazim dalam regulasi produk teknologi, agar korban tidak kehilangan forum pemulihan akibat sengketa internal antara bank dan vendor mengenai pihak yang bertanggung jawab atas kegagalan deteksi. Unsur ini secara langsung menjawab gap pertanggungjawaban korporasi-vendor yang diidentifikasi sebelumnya.
- Penguatan standar pembuktian forensik digital melalui pedoman teknis yang diakui pengadilan, termasuk sertifikasi laboratorium forensik digital dan keterangan ahli AI sebagai alat bukti yang sah, untuk mengatasi gap pembuktian yang menjadi titik lemah penegakan hukum saat ini.

Keempat unsur tersebut sejalan dengan, namun sekaligus melampaui, arah kebijakan yang saat ini ditempuh pemerintah. Rencana penerbitan dua Rancangan Perpres mengenai peta jalan dan etika AI pada tahun 2026 dapat dipandang sebagai langkah awal yang positif untuk membangun kesadaran tata kelola, tetapi tidak boleh diperlakukan sebagai titik akhir. Tanpa payung undang-undang, risiko terbesar yang dihadapi adalah lahirnya tata kelola AI yang bersifat soft law atau sekadar pedoman etika tanpa daya paksa hukum yang memadai untuk

melindungi korban pemalsuan identitas berbasis AI, sehingga prinsip negara hukum dalam arti substantif—bukan sekadar formalitas adanya aturan tertulis—belum benar-benar terpenuhi.

4. KESIMPULAN

Kerangka hukum positif Indonesia saat ini—KUHP, UU ITE, dan ketentuan sektor jasa keuangan—pada dasarnya memadai untuk menjerat pelaku individual pemalsuan identitas berbasis AI dalam pembukaan rekening perbankan sebagai tindak pidana konvensional, namun belum memadai dalam tiga hal struktural: standar pembuktian forensik digital, distribusi tanggung jawab antara bank dan vendor teknologi AI ketika sistem gagal mendeteksi pemalsuan, serta koordinasi kelembagaan antar-otoritas pengawas. Lalu, model regulasi AI yang sesuai dengan prinsip negara hukum di Indonesia mensyaratkan agar norma inti tata kelola AI—klasifikasi risiko, kewajiban audit, dan sanksi—dituangkan dalam undang-undang, bukan semata Peraturan Presiden, sebagai konsekuensi dari asas legalitas formil dan pembagian kekuasaan; sementara pendekatan berbasis risiko (risk-based) sebagaimana dianut EU AI Act dapat diadaptasikan secara kontekstual untuk Indonesia, khususnya pada klasifikasi sistem verifikasi biometrik perbankan sebagai sistem berisiko tinggi.

Pembentuk undang-undang disarankan untuk mendorong agar Rancangan Undang-Undang tentang Kecerdasan Artifisial—bukan sekadar Peraturan Presiden—menjadi agenda legislasi nasional, dengan melibatkan partisipasi publik yang bermakna guna menghindari kesan bahwa proses penyusunan didominasi kepentingan bisnis maupun politik tertentu. Otoritas Jasa Keuangan dan Kementerian Komunikasi dan Digital disarankan segera menyusun mekanisme pelaporan insiden algoritmik satu pintu sebagai langkah jangka pendek yang tidak perlu menunggu pengesahan undang-undang baru, mengingat modus pemalsuan identitas berbasis AI dalam pembukaan rekening perbankan adalah risiko yang sudah nyata terjadi, bukan ancaman hipotetis di masa depan.

DAFTAR PUSTAKA

Peraturan Perundang-undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Pidana.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-Undang Republik Indonesia Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan.

Undang-Undang Republik Indonesia Nomor 13 Tahun 2022 tentang Perubahan Kedua atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act).

Buku, Jurnal, dan Sumber Lain

- Arvitto, R. S. (2025). Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP. *Jurnal Ilmiah Hukum dan Hak Asasi Manusia*, 4(2), 73–82.
- Gunawan, I. J., & Janisriwati, S. (2023). Legal Analysis on the Use of Deepfake Technology: Threats to Indonesian Banking Institutions. *Law and Justice*, 8(2), 192–210.
- Judijanto, L., Utama, A. S., & Setiyawan, H. (2025). Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia. *The Easta Journal Law and Human Rights*, 3(02), 101–109.
- Kristiyenda, Y. S., Faradila, J., & Basanova, C. (2025). Pencegahan Kejahatan Deepfake: Studi Kasus Terhadap Modus Penipuan Deepfake Prabowo Subianto Dalam Tawaran Bantuan Uang. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, 3(2), 149–164.
- Medeline, F., Rusmiati, E., & Ramadhani, R. H. (2022). Forensik Digital dalam Pembuktian Tindak Pidana Ujaran Kebencian di Media Sosial. *PAMPAS: Journal of Criminal Law*, 3(3), 310–325.
- Rama, B. G. A., Prasada, D. K., & Mahadewi, K. J. (2023). Urgensi Pengaturan Artificial Intelligence (AI) dalam Bidang Hukum Hak Cipta di Indonesia. *Jurnal Rechtsens*, 12(2), 209–224.
- Rasyidah, N. A., Aksay, M., & Akmal, M. F. (2024). Urgensi Pembuatan Regulasi Penggunaan AI (Artificial Intelligence) Di Indonesia. *Jurnal Penegakan Hukum Indonesia*, 5(1), 42–51.