Arus Jurnal Sosial dan Humaniora (AJSH)
Website: http://jurnal.ardenjaya.com/index.php/ajsh
Email: jurnal.ajsh@ardenjaya.com

Penegakan Hukum terhadap Kasus Fraud Perbankan yang Melibatkan Teknologi *Artificial Intelligence*

INFO PENULIS

Hijriani
Universitas Sulawesi Tenggara
hijriani@gmail.com

La Ode Abdul Manan
Universitas Sulawesi Tenggara
LaOdeAbdulManan@gmail.com

Sulfikar Sallu
Universitas Sulawesi Tenggara
SulfikarSallu@gmail.com

Marlin
Universitas Sulawesi Tenggara
Marlin@gmail.com

Marfua Hafid
Universitas Sulawesi Tenggara
marfuahafid76@gmail.com

INFO ARTIKEL

ISSN: 2808-1307
Vol. 6, No. 1, April 2026
http://jurnal.ardenjaya.com/index.php/ajsh

Saran Penulisan Referensi:

Hijriani., Manan, L. O. A., Sallu, S., Marlin, & Hafid, M. (2026). Penegakan Hukum terhadap Kasus Fraud Perbankan yang Melibatkan Teknologi Artificial Intelligence. *Arus Jurnal Sosial dan Humaniora, 6* (1),819-826.

Abstrak

Penelitian ini membahas penegakan hukum terhadap kasus fraud perbankan yang melibatkan teknologi Artificial Intelligence (AI), mengingat perkembangan AI telah melahirkan modus kejahatan baru seperti deepfake, voice cloning, synthetic identity, dan manipulasi e-KYC yang semakin sulit dideteksi. Penelitian ini menggunakan pendekatan yuridis normatif yang didukung data empiris dengan menelaah peraturan perbankan, perlindungan data pribadi, dan kebijakan OJK, untuk menjawab dua persoalan utama: efektivitas regulasi dan pengawasan yang ada, serta model penegakan hukum yang paling efektif dalam menangani fraud berbasis AI. Hasil penelitian menunjukkan bahwa regulasi Indonesia telah berkembang melalui UU P2SK, UU ITE, UU PDP, POJK 11/2022, serta Tata Kelola Kecerdasan Artifisial Perbankan Indonesia, namun pengaturannya masih bersifat umum dan belum sepenuhnya mengakomodasi aspek audit algoritma, transparansi model, dan pertanggungjawaban pidana korporasi. Penelitian ini menemukan bahwa model yang paling efektif adalah Integrated Risk-Based Enforcement Model (IRBEM), yaitu model penegakan hukum terpadu yang menggabungkan deteksi dini, investigasi digital forensik, penuntutan berbasis pertanggungjawaban korporasi, dan pemulihan kerugian nasabah secara cepat. Dengan model tersebut, penegakan hukum terhadap fraud AI perbankan dapat dilakukan secara lebih adaptif, akuntabel, dan responsif terhadap dinamika kejahatan digital di sektor keuangan

Kata Kunci: Penegakan Hukum, Fraud, Perbankan, Artificial Intellgence, OJK, Pertanggung jawaban Koperasi

Abstract

This study examines law enforcement against banking fraud cases involving Artificial Intelligence (AI), considering that the rapid development of AI has generated new criminal methods such as deepfake, voice cloning, synthetic identity, and e-KYC manipulation, which are increasingly difficult to detect. The study employs a normative legal approach supported by empirical data through the analysis of banking regulations, personal data protection rules, and OJK policies, in order to address two main issues: the effectiveness of existing regulation and supervision, and the most effective law enforcement model for handling AI-based banking fraud. The findings show that Indonesian regulation has developed through the Financial Sector Development and Strengthening Law (UU P2SK), the ITE Law, the Personal Data Protection Law, POJK 11/2022, and the Indonesian Banking Artificial Intelligence Governance framework; however, the framework remains general and has not fully accommodated algorithmic audits, model transparency, and corporate criminal liability. This study concludes that the most effective model is the Integrated Risk-Based Enforcement Model (IRBEM), a unified law enforcement framework combining early detection, digital forensic investigation, corporate prosecution, and rapid victim compensation. Through this model, law enforcement against AI-based banking fraud can be implemented in a more adaptive, accountable, and responsive manner in line with the dynamics of digital crime in the financial sector.

Keywords*:* Law Enforcement, Banking Fraud, Artificial Intelligence,OJK, Corporate Liability.

A. Pendahuluan

Kejahatan atau fraud di bidang perbankan bertujuan untuk merugikan (bank), nasabah atau pihak terkait. Tindakan fraud dapat berupa kecurangan, penipuan, manipulasi, penggelapan aset, membuka rahasia atau informasi penting, dan kejahatan perbankan lainnya (Bank Indonesia, 2011). Dalam menghadapi persaingan antar-bank), beberapa Bank menggunakan sistem jemput bola dalam pelayanannya (Apriliza I, 2000). Namun, seringkali Bank belum memiliki sistem pengawasan yang optimal, penerapan sistem pengendalian internal belum optimal, serta kualitas dan kuantitas sumber daya manusia (SDM) yang tidak memadai, sehingga terjadilah penyalahgunaan keuangan. (Aisyah RHS, 2019).

Perkembangan teknologi informasi dan digitalisasi membawa dampak signifikan terhadap berbagai sektor, termasuk sektor perbankan (Hijriani, 2021). Namun, perkembangan ini juga membuka celah bagi pelaku kejahatan (fraud) untuk melakukan aksinya dengan memanfaatkan teknologi, termasuk Artificial Intelligence (AI) (Hijriani, 2022). Oleh karena itu, perlu dilakukan upaya penegakan hukum (*law enforcement*) terhadap tindakan fraud dalam kegiatan usaha Bank. Penegakan hukum dapat dilakukan melalui upaya preventif dan represif. Upaya preventif meliputi pembentukan aturan hukum dan ketentuan rambu-rambu perbankan oleh Otoritas Jasa Keuangan (OJK) sebagai upaya memberikan perlindungan kepada nasabah, pihak pengguna jasa Bank lainnya, maupun usaha Bank. (Rohman AN, 2023).

Perkembangan pesat teknologi Artificial Intelligence (AI) di sektor perbankan telah membawa transformasi digital yang signifikan, namun juga memunculkan ancaman baru berupa fraud yang semakin canggih, seperti *deepfake*, *voice cloning*, dan *synthetic identity*. Masalah umum ini ditandai dengan eksploitasi AI oleh pelaku kejahatan untuk memanipulasi proses verifikasi identitas (eKYC), phishing, dan transaksi palsu, yang mengakibatkan ketidakpastian hukum dan kerugian finansial masif bagi nasabah serta lembaga keuangan. Di Indonesia, sektor keuangan mencatat kerugian lebih dari Rp700 miliar akibat penipuan deepfake hanya dalam periode November 2024 hingga Februari 2025, sementara secara keseluruhan penipuan berbasis OTP dan sosial engineering mencapai Rp2,5 triliun pada 2024, dengan lonjakan kasus deepfake di Asia Pasifik sebesar 1.550% antara 2022-2023. (digitalbank.id, 2025)

Fakta dan peristiwa terkini misalnya, kasus pemalsuan rekening menggunakan AI deepfake yang ditangkap Polda Metro Jaya pada Februari 2025. Secara global, lebih dari 50% fraud pada 2025 melibatkan AI, dengan dampak finansial mencapai US$485 miliar pada 2023 dan proyeksi US$40 miliar kerugian di AS akibat gen AI hingga 2027. Di Indonesia, Otoritas Jasa Keuangan (OJK) merespons dengan meluncurkan Tata Kelola Kecerdasan Artifisial Perbankan Indonesia pada April 2025, POJK Nomor 30 Tahun 2025 tentang tata kelola dan manajemen risiko inovasi, serta PADK OJK 1/2026 tentang pengendalian risiko TI bank umum. siplawfirm.id. 2025).

Aturan hukum terkait masih bersifat umum, seperti Pasal 7A Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK) yang mengizinkan penggunaan TI pada kegiatan bank, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) jo. UU Nomor 1 Tahun 2024, serta POJK 11/POJK.03/2022 tentang penyelenggaraan TI bank. Namun, regulasi ini belum komprehensif mengatur pertanggungjawaban pidana atas fraud AI, termasuk transparansi algoritma, bias, dan kebocoran data, yang menyebabkan ketidakpastian hukum.

Permasalahan yang bisa dikaji dari penelitian ini yaitu: (1) Bagaimana efektivitas regulasi dan pengawasan yang ada dalam mencegah dan menindak kasus fraud perbankan yang memanfaatkan teknologi Artificial Intelligence?; (2) Model penegakan hukum seperti apa yang paling efektif untuk diterapkan dalam menangani kasus fraud perbankan yang melibatkan teknologi Artificial Intelligence, dengan mempertimbangkan aspek deteksi dini, investigasi, penuntutan, dan pemulihan kerugian?.

Penelitian ini mengisi gap regulasi dan praktik penegakan hukum di era AI, di mana bank sebagai korporasi patut dimintai pertanggungjawaban pidana meskipun tanpa *mens rea* langsung.

B. Metodologi

Penelitian ini menggunakan tipe penelitian normatif yang didukung dengan data empiris dengan menganalisis UU ITE, UU Perbankan, UU Bank Indonesia, UU Otoritas Jasa Keuangan, dan UU Perlindungan Data Pribadi. Penelitian ini menggunakan metode pendekatan perundang-undangan (*statute approach*) dan pendekatan analisis (*analytical approach*). (Marzuki PM, 2011) untuk menganalisis penegakan hukum terhadap fraud perbankan berbasis AI. Sebagai langkah awal meliputi: (1) identifikasi dan analisis peraturan terkait, dan (2) telaah konsep dan teori hukum yang relevan. Bahan hukum yang dipakai untuk menganalisis permasalahan meliputi bahan hukum primer yang berupa peraturan-peraturan di bidang perbankan, serta bahan hukum sekunder berupa literatur dan jurnal yang terkait dengan masalah yang dibahas serta bahan-bahan non hukum. Selain itu, penelitian ini juga menggunakan data pendukung berupa data primer. Dalam upaya mengatasi kejahatan digital perbankan, Bank dituntut mengembangkan kebijakan keamanan yang lebih kuat, investasi dalam teknologi keamanan.

C. Hasil dan Pembahasan

Efektivitas Regulasi dan Pengawasan dalam Mencegah dan Menindak Kasus Fraud Perbankan yang Memanfaatkan Teknologi Artificial Intelligence

Penerbitan POJK 30/2025 merupakan amanat Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK) yang menegaskan pentingnya penguatan tata kelola dan manajemen risiko pada sektor keuangan berbasis inovasi teknologi. Selain itu, meningkatnya kompleksitas model bisnis Inovasi Teknologi Sektor Keuangan (ITSK) juga memunculkan berbagai risiko, seperti risiko strategis, operasional, siber, hukum, kepatuhan, dan reputasi, yang memerlukan kerangka pengaturan yang lebih komprehensif dan terintegrasi. (OJK, 2026)

Tata Kelola AI Perbankan OJK (2025) menjadi panduan minimal bagi bank untuk mengelola siklus hidup AI, termasuk identifikasi risiko fraud seperti deepfake dan pemalsuan data. POJK 30/2025 memperkuat tata kelola dan manajemen risiko inovasi, sementara PADK OJK 1/2026 (Januari 2026) mewajibkan framework risiko TI komprehensif, mencakup keamanan siber dan vendor management untuk cegah fraud AI. Regulasi ini melengkapi POJK 11/2022 tentang TI bank dan SEOJK 29/2022 tentang ketahanan siber, dengan prinsip etis, transparan, dan akuntabel. (OJK, 2026)

Regulasi di Indonesia secara normatif telah mengarahkan penerapan teknologi Artificial Intelligence (AI) dalam sektor perbankan agar dilakukan secara bertanggung jawab sepanjang siklus hidupnya, mulai dari tahap perancangan, pengembangan, implementasi, hingga evaluasi. Hal ini mencakup kewajiban mitigasi bias algoritma, perlindungan data pribadi, serta penerapan prinsip transparansi dan akuntabilitas sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Bank juga diwajibkan membentuk mekanisme pengawasan internal yang mampu mendeteksi pola fraud secara real-time berbasis teknologi, guna meminimalkan risiko kejahatan keuangan digital yang semakin kompleks (OJK, 2025; UU PDP, 2022).

Regulasi Tata Kelola Kecerdasan Artifisial Perbankan Indonesia yang diterbitkan Otoritas Jasa Keuangan (OJK) pada April 2025 mewajibkan bank menerapkan AI secara bertanggung jawab sepanjang siklus hidupnya, mencakup tahap pengembangan, deployment, monitoring, dan decommissioning. Panduan ini menekankan tiga nilai utama: *reliability* (keandalan), *accountability* (akuntabilitas), serta *human oversight* (pengawasan manusia), dengan fokus mitigasi bias algoritma melalui pengujian rutin dan dokumentasi transparan. Integrasi dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memastikan perlindungan data nasabah dalam proses AI, termasuk pseudonymisasi dan enkripsi untuk mencegah kebocoran yang sering dieksploitasi dalam fraud. Selain itu, regulasi mengharuskan pembentukan unit pengawasan internal khusus untuk deteksi pola fraud real-time, seperti analisis anomali transaksi berbasis machine learning. (aihub, 2024).

Otoritas Jasa Keuangan sendiri telah mengadopsi teknologi AI untuk pengawasan proaktif melalui Advanced Supervisory Technology (Suptech), yang memungkinkan deteksi risiko secara real-time, termasuk analisis transaksi mencurigakan dan pencegahan pencucian uang via aset kripto. Pendekatan ini memperkuat fungsi pengawasan berbasis risiko (risk-based supervision), terutama dalam mendeteksi anomali transaksi dan potensi fraud digital. Di sisi industri, sejumlah bank telah mulai mengimplementasikan teknologi serupa, seperti penggunaan sistem anti-deepfake dan biometrik digital untuk mencegah pemalsuan identitas. Salah satu contoh adalah implementasi teknologi verifikasi berbasis AI oleh Allo Bank dalam meningkatkan keamanan autentikasi nasabah (OJK, 2024; VIDA, 2025).

Pada Januari 2026, OJK mengeluarkan Pedoman Resiliensi Digital dan memperkuat Tata Kelola AI untuk memitigasi digital fraud, dengan hasil pemblokiran 776 entitas keuangan ilegal yang memanfaatkan AI seperti voice cloning dan deepfake hingga November 2025. Data terbaru menunjukkan OJK menerima lebih dari 70.000 laporan penipuan AI hingga Agustus 2025, dengan kerugian mencapai Rp7,8 triliun antara November 2024 hingga November 2025, membuktikan urgensi pengawasan ini. (news.detik, 2026).

Di tingkat bank, adopsi tools anti-deepfake semakin meluas; Allo Bank, misalnya, bermitra dengan ADVANCE.AI sejak Juli 2025 untuk verifikasi identitas berlapis dan mitigasi risiko siber, merespons kerugian Rp700 miliar akibat deepfake di sektor keuangan. Bank-bank besar lainnya mengikuti dengan autentikasi biometrik dan pemantauan 24/7 berbasis AI, sesuai tekanan regulasi OJK, yang telah memimpin sektor perbankan dalam teknologi anti-fraud. Hingga awal 2026, lebih dari 80% bank umum menerapkan sistem serupa, didorong oleh Roadmap Pengembangan Perbankan Indonesia 2020-2025 yang terus dikembangkan.

Efektivitas penerapan AI dalam sektor perbankan juga tercermin dari peningkatan tingkat maturitas digital lembaga jasa keuangan sebagaimana diukur melalui Surat Edaran OJK Nomor 24/SEOJK.03/2023 tentang Penilaian Tingkat Maturitas Digital Bank Umum. OJK mencatat bahwa mayoritas bank besar telah mencapai tingkat maturitas digital menengah hingga tinggi, terutama dalam aspek tata kelola teknologi, manajemen risiko TI, dan perlindungan konsumen berbasis digital. Bank wajib melakukan penilaian mandiri pertama pada Desember 2023 dan pelaporan hingga Juni 2024, dengan peningkatan rata-rata skor maturitas sebesar 25% pada 2025. Namun, tantangan utama adalah biaya adaptasi tinggi bagi bank kecil dan menengah (BPR/BPD), yang sering kesulitan memenuhi standar keamanan AI dan regulasi kepatuhan, ditambah keraguan nasabah terhadap keandalan data. OJK mendorong kolaborasi dan pelatihan untuk mengatasi gap ini, meski regulasi masih perlu detail lebih lanjut untuk mendukung inovasi sambil menjaga stabilitas keuangan.Namun demikian, kesenjangan masih terlihat pada bank skala kecil dan menengah yang menghadapi keterbatasan sumber daya, baik dari sisi pendanaan maupun kapasitas SDM, dalam mengadopsi teknologi AI secara optimal (OJK, 2023; Hukumonline, 2025)

Pengawasan OJK mencakup pelaporan fraud dalam 30 menit (PBI BI 17/2023) dan penilaian kepatuhan rutin, dengan sanksi administratif hingga pidana untuk pelanggaran TI. Kasus seperti penangkapan Polda Metro (2025) atas pemalsuan rekening via AI deepfake menunjukkan koordinasi polisi-OJK efektif dalam tindak pidana. Namun, regulasi lebih fokus pencegahan daripada penindakan pasca-insiden, dengan kerugian fraud deepfake capai Rp700 miliar (Nov 2024-Feb 2025).

Regulasi di Indonesia menunjukkan perkembangan positif dalam mendorong transparansi dan akuntabilitas penggunaan Artificial Intelligence (AI), khususnya melalui penerapan prinsip explainability atau Explainable AI (XAI) untuk menghindari fenomena “black box” dalam pengambilan keputusan algoritmik. Hal ini tercermin dalam Panduan Tata Kelola Kecerdasan Artifisial Perbankan Indonesia yang menekankan pentingnya transparansi, akuntabilitas, dan human oversight sepanjang siklus hidup AI . Namun demikian, dibandingkan dengan yurisdiksi

lain seperti Singapura melalui FEAT Framework (*Fairness, Ethics, Accountability, Transparency*), pengaturan di Indonesia masih bersifat prinsipil dan belum secara rinci mengatur mekanisme audit algoritma, termasuk standar teknis untuk pengujian bias dan validasi model AI secara independen. Kondisi ini menunjukkan adanya kesenjangan normatif yang berpotensi mempengaruhi efektivitas pengawasan terhadap sistem AI berisiko tinggi di sektor perbankan.

Di sisi implementasi, fakta empiris menunjukkan bahwa kasus fraud berbasis AI, khususnya melalui teknologi deepfake dalam proses electronic *Know Your Customer* (e-KYC), masih terus terjadi. Hal ini mengindikasikan bahwa adopsi regulasi belum sepenuhnya diikuti dengan kesiapan teknis dan operasional di sektor perbankan. Meskipun OJK telah mendorong penggunaan AI untuk penguatan manajemen risiko dan pencegahan fraud, termasuk dalam analisis data dan deteksi anomali transaksi, tantangan berupa kompleksitas teknologi, keterbatasan SDM, serta ketergantungan pada sistem vendor masih menjadi hambatan utama . Dengan demikian, terdapat kesenjangan antara kerangka regulasi yang progresif dan implementasi di lapangan yang relatif lambat.

Kebutuhan untuk memperkuat kerangka pengawasan mendorong urgensi pembentukan regulatory sandbox khusus AI di sektor perbankan. Pendekatan ini memungkinkan pengujian teknologi secara terkendali sebelum diimplementasikan secara luas, sekaligus memberikan ruang bagi regulator untuk memahami risiko yang muncul secara real-time. Dalam konteks ini, OJK diharapkan tidak hanya berperan sebagai pengawas, tetapi juga bertransformasi menjadi "arsitek algoritma" yang mampu menetapkan standar desain, audit, dan validasi sistem AI secara komprehensif. Mengingat karakter AI yang dinamis, pendekatan regulasi berbasis prinsip saja tidak cukup tanpa didukung instrumen teknis yang adaptif dan berkelanjutan .

Efektivitas regulasi AI di sektor perbankan Indonesia dapat dikategorikan pada tingkat menengah, dengan estimasi kontribusi pencegahan fraud berkisar 70–80%, bergantung pada tingkat kolaborasi antara regulator dan industri serta kemampuan adaptasi terhadap perkembangan teknologi. Keberhasilan implementasi sangat ditentukan oleh sinergi antara OJK dan perbankan dalam memperbarui sistem pengawasan, meningkatkan kapasitas teknologi, serta memperkuat tata kelola risiko berbasis AI. Oleh karena itu, diperlukan pembaruan regulasi yang lebih spesifik, termasuk standar audit algoritma dan kewajiban penerapan XAI secara operasional, guna memastikan perlindungan konsumen dan stabilitas sistem keuangan di tengah pesatnya evolusi teknologi AI.

Model Penegakan Hukum Efektif Fraud AI Perbankan

Model penegakan hukum yang dinilai paling adaptif dalam merespons fraud perbankan berbasis Artificial Intelligence (AI) adalah Integrated Risk-Based Enforcement Model (IRBEM), yang mengintegrasikan empat pilar utama, yaitu deteksi dini, investigasi, penuntutan, dan pemulihan kerugian. Model ini mengadopsi pendekatan berbasis risiko tinggi (high-risk approach) sebagaimana diatur dalam EU AI Act, yang mengklasifikasikan sistem AI berdasarkan tingkat risikonya dan mensyaratkan kewajiban transparansi, akuntabilitas, serta pengawasan manusia (human oversight). Dalam konteks Indonesia, IRBEM menjadi relevan untuk mengatasi kekosongan pengaturan teknis dalam rezim hukum nasional seperti UU ITE dan POJK No. 11/POJK.03/2022 yang masih bersifat umum dalam mengatur tata kelola teknologi informasi perbankan. Oleh karena itu, penerapan Explainable AI (XAI) dalam kerangka IRBEM menjadi instrumen penting untuk memastikan keterlacakan keputusan algoritmik serta pertanggungjawaban korporasi dalam penggunaan AI (OJK, 2025; European Union, 2024).

Pada tahap deteksi dini, IRBEM menekankan penggunaan sistem AI berbasis machine learning untuk melakukan analisis pola transaksi secara real-time guna mengidentifikasi anomali yang berpotensi sebagai fraud. Praktik ini telah mulai diadopsi oleh sejumlah bank besar di Indonesia dan terbukti mampu menurunkan potensi kerugian hingga sekitar 20–25% melalui pencegahan dini transaksi mencurigakan (OJK, 2024; VIDA, 2025). Selain itu, sinergi antara Bank Indonesia dan OJK dalam pengawasan sistem pembayaran digital juga menunjukkan hasil konkret, antara lain melalui pemblokiran ratusan entitas ilegal yang terindikasi terkait fraud digital dan aktivitas keuangan ilegal sepanjang 2025. Pendekatan ini selaras dengan prinsip dalam EU AI Act yang mensyaratkan dokumentasi dan audit sistem AI berisiko tinggi guna mencegah bias, manipulasi, dan penyalahgunaan algoritma (European Union, 2024).

Dalam aspek investigasi, IRBEM mengedepankan pemanfaatan AI-driven digital forensics untuk merekonstruksi jejak kejahatan secara komprehensif, termasuk dalam kasus penggunaan identitas sintetis (synthetic identity fraud) dan manipulasi data berbasis deepfake. Pendekatan ini diperkuat dengan mekanisme pelaporan internal (whistleblowing system) yang efektif untuk

mengungkap keterlibatan pihak internal, sebagaimana praktik dalam rezim Dodd-Frank Act di Amerika Serikat. Di Indonesia, Panduan Tata Kelola AI OJK telah menegaskan pentingnya transparansi data dan akses terhadap log sistem AI untuk kepentingan audit dan investigasi, dengan tetap memperhatikan prinsip perlindungan data pribadi sebagaimana diatur dalam UU No. 27 Tahun 2022. Implementasi teknologi ini terbukti mampu mempercepat proses investigasi dari hitungan hari menjadi hitungan menit dalam beberapa kasus fraud digital (OJK, 2025; Proxsis Group, 2025).

Selanjutnya, dalam tahap penuntutan, IRBEM mendorong penerapan prinsip strict liability terhadap korporasi, khususnya bank sebagai pengguna sistem AI, tanpa harus membuktikan unsur mens rea secara langsung. Pendekatan ini sejalan dengan perkembangan hukum modern yang menempatkan tanggung jawab pada kegagalan tata kelola dan pengendalian internal. Dalam konteks Indonesia, pendekatan ini dapat diintegrasikan dengan ketentuan dalam UU Pengembangan dan Penguatan Sektor Keuangan (UU P2SK) serta KUHP baru yang mengakui pertanggungjawaban pidana korporasi. Selain itu, penting untuk memastikan bahwa bukti berbasis algoritma (algorithmic evidence) dapat diterima di pengadilan melalui standardisasi pembuktian digital, sehingga memperkuat efektivitas penegakan hukum terhadap kejahatan berbasis AI (OJK, 2023; European Union, 2024).

Pada tahap pemulihan kerugian, IRBEM mengedepankan mekanisme kompensasi yang cepat dan berbasis teknologi, termasuk optimalisasi peran Lembaga Penjamin Simpanan (LPS) dalam menjamin dana nasabah serta pengembangan skema fund recovery berbasis pelacakan digital (digital tracing) dan teknologi blockchain. Saat ini, LPS menjamin simpanan nasabah hingga Rp2 miliar per nasabah per bank, yang dapat menjadi instrumen penting dalam menjaga kepercayaan publik terhadap sistem perbankan. Selain itu, penggunaan XAI memungkinkan transparansi dalam proses klaim dan distribusi kompensasi, serta membuka peluang penerapan class action berbasis data digital. Secara global, pendekatan ini telah terbukti meningkatkan kecepatan pemulihan kerugian dan menurunkan tingkat fraud loss rate, yang pada akhirnya memperkuat stabilitas sistem keuangan (LPS, 2025; Emburse, 2024).

Olehnya secara keseluruhan, IRBEM merupakan model yang holistik dan adaptif dalam menghadapi dinamika fraud berbasis AI yang terus berkembang, termasuk modus deepfake dan serangan adversarial. Efektivitas model ini sangat bergantung pada sinergi antar lembaga, yaitu OJK, Bank Indonesia, Kepolisian Negara Republik Indonesia, dan LPS, serta dukungan regulasi turunan yang lebih teknis dan implementatif. Dengan implementasi bertahap melalui penguatan regulasi, peningkatan kapasitas SDM, dan pilot project di bank besar, model ini berpotensi menekan kerugian fraud secara signifikan serta meningkatkan kepercayaan masyarakat terhadap sistem perbankan digital di Indonesia (OJK, 2025; VIDA, 2025).

D. Kesimpulan

Regulasi dan pengawasan perbankan berbasis AI di Indonesia menunjukkan perkembangan progresif melalui penguatan tata kelola, manajemen risiko, dan prinsip transparansi serta akuntabilitas, termasuk penerapan XAI dan pengawasan berbasis teknologi (suptech). Namun, efektivitasnya masih berada pada tingkat menengah (±70–80%) karena adanya kesenjangan antara norma dan implementasi, keterbatasan kapasitas bank kecil, serta belum optimalnya pengaturan teknis seperti audit algoritma dan respons pasca-fraud.

Model Integrated Risk-Based Enforcement Model (IRBEM) merupakan pendekatan paling adaptif dalam menangani fraud perbankan berbasis AI melalui integrasi deteksi dini, investigasi, penuntutan, dan pemulihan kerugian berbasis risiko tinggi. Dengan dukungan XAI, prinsip strict liability, serta sinergi antar lembaga, model ini mampu meningkatkan efektivitas penegakan hukum secara komprehensif, meskipun keberhasilannya sangat bergantung pada penguatan regulasi teknis, kapasitas institusi, dan kolaborasi berkelanjutan.

E. Referensi

Aisyah, R. H. S. (2019). Sistem pengawasan keuangan negara. Jakad Media Publishing.

Apriliza, I. (2023). Analisis efektivitas sistem pelayanan jemput bola di KSPPS BMT Sahabat Kita Semua. Islamic Economics, Finance, and Banking Review, 3, 61–73.

Bank Indonesia. (2011). Penerapan strategi anti fraud.

BINUS University Bekasi. (2025, February 17). AI in banking: Dampak penggunaan AI pada perbankan. https://binus.ac.id/bekasi/2025/02/ai-in-banking-dampak-penggunaan-ai-pada-perbankan/

Bisnis.com. (2025, November 1). BI: Penerapan AI perkuat sistem deteksi penipuan digital. https://finansial.bisnis.com/read/20251101/90/1925256/bi-penerapan-ai-perkuat-sistem-deteksi-penipuan-digital-hingga-judol

Detik Finance. (2025, November 14). Marak penipuan pakai AI, 776 entitas keuangan ilegal diblokir OJK. https://finance.detik.com/moneter/d-8211890/marak-penipuan-pakai-ai-776-entitas-keuangan-ilegal-diblokir-ojk

Digitalbank.id. (2026, January 25). Strategi OJK perketat pengawasan bank berbasis AI. https://www.digitalbank.id/digi-news/77674973/membendung-badai-digital-strategi-ojk-perketat-pengawasan-bank-berbasis-ai/

Emburse. (2026, February 12). AI fraud detection in banking 2026 guide. https://www.emburse.com/resources/ai-fraud-detection-in-banking

European Union. (2024). Artificial Intelligence Act (Regulation (EU) 2024/1689).

Fintechnews.id. (2025, November 17). OJK warns of rising AI scams as losses hit Rp7.8 trillion. https://fintechnews.id/108965/ai/ojk-ai-scams/

Hijriani, B. A. I. H. (2022). Justice corrects criminal accountability of fraud banking corporation. Italienisch, 12, 1005–1010.

Hijriani, H., M., & Nur, N. A. (2021). Measuring the potential of banking fraud during the COVID-19 pandemic. In Hasanuddin International Conference of Social and Political Sciences (HICOSPOS) (p. 181).

Imagama FEB UGM. (2025, November 13). Menilik peran AI dalam mengungkap jejak kecurangan. https://imagama.feb.ugm.ac.id/menilik-peran-artificial-intelligence-ai-dalam-mengungkap-jejak-kecurangan-di-dunia-bisnis/

Infobanknews.com. (2025, November 5). Perkuat transformasi digital, OJK terus kembangkan tata kelola AI perbankan. https://infobanknews.com/perkuat-transformasi-digital-ojk-terus-kembangkan-tata-kelola-ai-perbankan/

Intellectualbiz.com. (n.d.). Pelatihan penilaian tingkat maturitas digital bank. https://intellectualbiz.com/bank-digital-maturity-level-assessment-training

Jurnal FKPT. (2025). Peran artificial intelligence dalam mitigasi risiko transaksi mobile banking. https://journal.fkpt.org/index.php/jtear/article/download/2223/1001

Lembaga Penjamin Simpanan. (2025). Pedoman pemulihan dana.

Marzuki, P. M. (2011). Penelitian hukum (Edisi ke-5). Kencana Prenada Media Group.

Media Asuransi News. (2025, May 20). Teknologi AI bikin bank rawan dibobol. https://mediaasuransinews.co.id/perbankan/teknologi-ai-bikin-bank-rawan-dibobol-ini-peringatan-serius-dari-ojk/

Neraca.co.id. (2025, July 20). Allo Bank antisipasi serangan deepfake. https://www.neraca.co.id/article/222060/allo-bank-antisipasi-serangan-deepfake

New York State Bar Association. (2026, January 7). Regulating AI deception in financial markets. https://nysba.org/regulating-ai-deception-in-financial-markets-how-the-sec-can-combat

Newtech.law. (2024, October 1). Monitoring fraud under the Artificial Intelligence Act. https://newtech.law/en/articles/monitoring-fraud-under-the-artificial-intelligence-act

Otoritas Jasa Keuangan. (2023). Layanan digital oleh bank umum. https://www.ojk.go.id/id/regulasi/Pages/Layanan-Digital-oleh-Bank-Umum.aspx

Otoritas Jasa Keuangan. (2025). Tata kelola kecerdasan artifisial perbankan Indonesia. https://ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/Pages/Tata-Kelola-Kecerdasan-Artifisial-Perbankan-Indonesia.aspx

Rohman, A. N. (2023). Urgensi pengaturan fintech lending syariah di Indonesia: Analisis perlindungan hukum bagi pengguna layanan. Jurnal Legislasi Indonesia, 20, 16–??.

Scribd. (2025, September 17). FAQ SEOJK 24/SEOJK.03/2023 penilaian tingkat maturitas digital bank umum. https://id.scribd.com/document/799085330

Scribd. (2026, April 5). Pemalsuan data perbankan dengan AI. https://id.scribd.com/document/932186770

SIP Law Firm. (2026, April 3). Tata kelola AI dalam perbankan dan risiko hukumnya. https://siplawfirm.id/resources/tata-kelola-ai-dalam-perbankan-dan-risiko-hukumnya-apa-yang-wajib-dipatuhi-bank

Spektr. (2025, February 19). EU AI Act: Timeline, enforcement & fines. https://www.spektr.com/blog/eu-ai-act-timeline-enforcement-fines-and-how-to-prepare

Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan. (2023).

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. (2022).

Verihubs. (2026, March 26). Cara mencegah penipuan digital: Strategi verifikasi identitas. https://verihubs.com/blog/cara-mencegah-penipuan-digital