

**ARTIFICIAL INTELLIGENCE-ASSISTED BUSINESS CRIME:
TANTANGAN REGULASI HUKUM PIDANA DI INDONESIA
ARTIFICIAL INTELLIGENCE-ASSISTED BUSINESS CRIME:
CHALLENGES FOR CRIMINAL LAW REGULATION IN INDONESIA**

Aida Ardini dan Pudjianto Gondosasmito

**PUI-PT Criminal Law and Green Economy, Faculty of Law, Universitas Prima
Indonesia, Medan**

Korespondensi Penulis : aidardini@unprimdn.ac.id, gondosasmitopudjianto@gmail.com

Citation Structure Recommendation :

Ardini, Aida dan Pudjianto Gondosasmito. *Artificial Intelligence-Assisted Business Crime:
Tantangan Regulasi Hukum Pidana di Indonesia*. Rewang Rencang : Jurnal Hukum Lex
Generalis. Vol.7. No.7 (2026).

ABSTRAK

Artificial Intelligence (AI) telah mentransformasi kejahatan bisnis menjadi kriminalitas berbasis algoritma yang menantang hukum pidana konvensional di Indonesia. Penelitian ini mengkaji kesenjangan regulasi dalam penjatuhan pertanggungjawaban pidana korporasi terhadap AI-assisted business crime melalui metode penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, komparatif dan kasus. Hasil penelitian menunjukkan tiga kelemahan utama, yaitu ketiadaan norma pidana khusus AI, keterbatasan doktrin mens rea dan lemahnya kewajiban tata kelola AI korporasi. Penelitian ini menegaskan perlunya pergeseran dari kesalahan individual menuju kegagalan tata kelola algoritmik dalam penjatuhan pidana korporasi.

Kata Kunci: Artificial Intelligence, Kejahatan Bisnis, Pertanggungjawaban Pidana Korporasi

ABSTRACT

Artificial Intelligence (AI) has transformed business crime into algorithm-driven misconduct that challenges conventional criminal law in Indonesia. This study examines regulatory gaps in imposing corporate criminal liability for AI-assisted business crime using normative legal research with statutory, conceptual, comparative and case approaches. The findings reveal three major deficiencies: the absence of AI-specific criminal norms, limitations of the traditional mens rea doctrine and weak corporate AI governance obligations. This study argues that AI adoption in criminal law requires a shift from individual fault to algorithmic governance failure, particularly in determining corporate criminal punishment and strengthening accountability in AI-driven business crimes.

Keywords: Artificial Intelligence, AI-Assisted Business Crime, Corporate Criminal Liability, Criminal Law Reform, Indonesia.

A. PENDAHULUAN

Transformasi ekonomi digital dalam satu dekade terakhir telah mengubah secara fundamental cara entitas bisnis beroperasi, mengambil keputusan dan menciptakan nilai ekonomi. Di antara berbagai inovasi teknologi yang mendorong perubahan tersebut, *Artificial Intelligence* (AI) menempati posisi yang sangat strategis karena kemampuannya untuk memproses data dalam skala besar, membangun prediksi berbasis pola, serta menghasilkan keputusan semi-otomatis maupun otonom dalam aktivitas bisnis. Integrasi AI ke dalam sektor keuangan, perdagangan elektronik, perbankan, asuransi, hingga tata kelola korporasi telah meningkatkan efisiensi operasional secara signifikan. Namun, kemajuan teknologi ini juga menghadirkan paradoks regulatif: instrumen yang dirancang untuk meningkatkan produktivitas bisnis pada saat yang sama mampu menjadi medium baru bagi praktik kejahatan ekonomi yang semakin kompleks.

Diskursus mengenai kejahatan bisnis secara tradisional bertumpu pada gagasan *white-collar crime* yang diperkenalkan oleh Edwin Sutherland, yakni kejahatan yang dilakukan oleh individu atau entitas yang memiliki status sosial tinggi dalam aktivitas pekerjaan atau bisnis.¹ Meski kerangka tersebut masih relevan, lanskap kontemporer menunjukkan bahwa tipologi kejahatan bisnis telah mengalami pergeseran struktural. Kejahatan bisnis tidak lagi semata bergantung pada manipulasi dokumen, pemalsuan laporan keuangan, atau kolusi antar pelaku ekonomi. Kehadiran AI telah memperluas spektrum modus operandi melalui otomatisasi penipuan, manipulasi algoritmik pasar, pemrosesan identitas sintesis, serta rekayasa informasi digital yang sulit dibedakan dari data autentik.² Pergeseran ini menunjukkan bahwa evolusi kejahatan bisnis bukan hanya perubahan instrumen, melainkan transformasi epistemologis mengenai bagaimana niat jahat (*criminal intent*) dapat diwujudkan melalui sistem komputasional.

¹ Imran Ali Mangrio dan Liaquat Ali Abro, *Multi Faceted White Collar Crime Eating Country's Economic Fabric Like Termite*, Al Meezan Research Journal of Social Sciences, Vol.2, No.2 (2022).

² Zulfikar Hasan dan Diska Sendi Marisna, *Artificial Intelligence: Making Crime Easier in The World of Finance?*, AL-ARBAH: Journal of Islamic Finance and Banking, Vol.6, No.2 (2024).

Salah satu perkembangan yang paling mengkhawatirkan adalah meningkatnya penggunaan AI sebagai crime enabler dalam skema penipuan finansial. Sistem pembelajaran mesin kini dapat digunakan untuk mengidentifikasi celah perilaku konsumen, memetakan kerentanan psikologis investor dan menghasilkan skenario manipulatif dengan tingkat personalisasi yang jauh melampaui kapasitas manusia. Praktik deepfake financial fraud, misalnya, menunjukkan bagaimana AI mampu mereplikasi suara atau visual eksekutif perusahaan untuk memberikan instruksi transfer dana palsu yang secara kasatmata tampak autentik. Deepfake Dalam konteks ini, AI tidak lagi berfungsi sebagai alat pasif, tetapi sebagai akselerator risiko kriminal yang meningkatkan skala, presisi dan efektivitas kejahatan bisnis.³

Urgensi pengaturan AI dalam hukum pidana semakin nyata ketika berbagai yurisdiksi mulai menghadapi kasus kriminal yang melibatkan sistem AI. Salah satu contoh yang banyak menjadi perhatian global adalah penggunaan teknologi deepfake untuk penipuan finansial korporasi, di mana pelaku memalsukan suara eksekutif perusahaan melalui AI guna menginstruksikan transfer dana dalam jumlah besar. Kasus semacam ini menunjukkan bahwa AI tidak lagi hanya berfungsi sebagai instrumen pendukung aktivitas ekonomi, tetapi telah berkembang menjadi medium yang dapat memfasilitasi fraud, manipulasi pasar dan pencucian uang secara lebih canggih. Dalam konteks Indonesia, potensi penyalahgunaan serupa semakin tinggi seiring pesatnya adopsi AI dalam sektor perbankan, fintech dan perdagangan digital. Meskipun demikian, hingga saat ini belum terdapat pengaturan pidana yang secara spesifik mengatur atribusi pertanggungjawaban atas tindak pidana yang dihasilkan atau difasilitasi oleh sistem AI.⁴

Permasalahan menjadi semakin kompleks ketika AI diintegrasikan ke dalam struktur korporasi modern. Berbeda dari kejahatan individual, business crime berbasis AI sering kali muncul dari adanya interaksi antara sistem teknologi,

³ Nurulhuda Irawati, Ismansyah dan Nani Mulyati, *Pertanggungjawaban Pidana Deepfake Porn Berbasis AI: Studi Perbandingan dan Implikasi Global*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.7, No.1 (2026).

⁴ Marshella Cenyvesta dan Ariawan Gunadi, *Konsep Tanggung Jawab Negara terhadap Kewajiban Melindungi Data Pribadi Masyarakat di Indonesia (Studi Kasus Kebocoran Data NPWP Masyarakat Indonesia)*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.5, No.12 (2024).

kebijakan internal perusahaan, model bisnis dan budaya organisasi. Akibatnya, hubungan kausal antara tindakan kriminal dan subjek hukum menjadi kabur. Ketika algoritma perdagangan otomatis melakukan manipulasi harga pasar, pertanyaan hukum yang muncul bukan sekadar apakah telah terjadi pelanggaran, melainkan siapa yang dapat dimintai pertanggungjawaban pidana: pengembang sistem, operator algoritma, direksi perusahaan, atau korporasi itu sendiri.⁵ Kompleksitas ini memperlihatkan keterbatasan paradigma hukum pidana klasik yang dibangun atas asumsi bahwa pelaku tindak pidana selalu merupakan subjek yang memiliki kehendak sadar, niat dan kontrol langsung terhadap perbuatannya.

Di titik inilah muncul *theoretical gap* yang signifikan. Literatur tentang AI umumnya berkembang dalam ranah etika teknologi dan tata kelola digital, sedangkan kajian tentang business crime lebih banyak berfokus pada fraud korporasi, anti-money laundering dan financial misconduct.⁶ Money Laundering Persinggungan antara kedua bidang tersebut khususnya mengenai konstruksi pertanggungjawaban pidana ketika AI menjadi medium kejahatan korporasi masih relatif terbatas, terutama dalam konteks negara berkembang. Dengan demikian, perdebatan akademik saat ini belum sepenuhnya menjawab bagaimana konsep kesalahan pidana (*mens rea*) dapat diterapkan pada kejahatan yang melibatkan sistem algoritmik semi-otonom.⁷

Sejumlah penelitian terdahulu telah mengkaji hubungan antara Artificial Intelligence (AI) dan hukum pidana, namun masih menyisakan ruang kajian yang signifikan. Fernández Llorca et al. (2022)⁸ menganalisis rezim pertanggungjawaban hukum dalam penggunaan AI dengan menitikberatkan pada problem pembuktian dan beban tanggung jawab atas kerugian yang dihasilkan sistem otonom, tetapi kajian tersebut lebih berorientasi pada kerangka liability umum dan belum membahas implikasinya dalam konteks kejahatan bisnis.

⁵ Thomas C. King, dkk., *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, Science and Engineering Ethics, Vol.26, No.1 (2020).

⁶ Rasji dan Rupertus Arvini Ngabut, *Filsafat Positivisme Hukum dalam Pemberantasan Pencucian Uang: Analisis Kepastian Hukum dan Implementasi di Indonesia*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.5, No.10 (2024).

⁷ Sonali dan Gunjan, *Human Agency and Machine Logic: Reassessing Mens Rea in The Age of Algorithmic Decision-Making*, In *From Mens Rea to Machine Rea: Reimagining Criminal Culpability in Digital Age*, Redshine Publication, Lunawada, 2025.

⁸ David Fernández Llorca, dkk., *Liability Regimes in the Age of AI: a Use-Case Driven Analysis of the Burden of Proof*, Journal of Artificial Intelligence Research, Vol.76 (2023).

Mongillo (2023)⁹ mengkaji kemungkinan penerapan doktrin pertanggungjawaban pidana korporasi terhadap AI-related crimes serta menyoroti berbagai hambatan konseptual dalam yurisdiksi Eropa, namun belum secara spesifik mengaitkannya dengan karakter business crime yang berbasis keuntungan ekonomi korporasi. Suseno et al. (2025)¹⁰ meneliti pengaturan cybercrime dalam rezim hukum pidana Indonesia dan menunjukkan adanya tantangan adaptasi hukum nasional terhadap kejahatan digital, tetapi belum menempatkan AI sebagai medium utama dalam konstruksi tindak pidana. Purnomo (2023)¹¹ membahas pertanggungjawaban pidana atas penggunaan AI dalam konteks hukum Indonesia, namun analisisnya masih bersifat umum dan belum menguraikan model pertanggungjawaban korporasi secara mendalam.

Berbeda dengan penelitian-penelitian tersebut, penelitian ini secara khusus memfokuskan analisis pada *AI-assisted business crime* dalam perspektif hukum pidana Indonesia dengan menempatkan korporasi sebagai aktor sentral dalam atribusi kesalahan pidana. Kebaruan penelitian ini terletak pada integrasi antara kajian business crime, Corporate Criminal Liability Theory dan reformasi hukum pidana berbasis tata kelola AI melalui pendekatan *algorithmic governance failure*. Pendekatan ini menawarkan model rekonstruksi pertanggungjawaban pidana korporasi yang lebih adaptif terhadap kriminalitas bisnis berbasis AI di Indonesia.

Pada level regulasi, Indonesia memang telah mulai merespons perkembangan AI melalui beberapa instrumen kebijakan, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial, serta Strategi Nasional Kecerdasan Artifisial 2020–2045 yang disusun oleh Badan Pengkajian dan Penerapan Teknologi.

Namun, instrumen-instrumen tersebut pada dasarnya masih berorientasi pada tata kelola etika, perlindungan data dan arah pengembangan teknologi,

⁹ Maklu-Online, *Corporate Criminal Liability for AI Related Crimes: Possible Legal Techniques and Obstacles*, diakses dari <https://www.maklu-online.eu/en/tijdschrift/ridp/2023/traditional-criminal-law-categories-and-ai-crisis/corporate-criminal-liability-ai-related-crimes-pos/>, diakses pada 5 Juli 2026.

¹⁰ Sigid Suseno, dkk., *Cybercrime in the New Criminal Code in Indonesia*, Cogent Social Sciences, Vol.11, No.1 (2025).

¹¹ Hadi Purnomo, *Criminal Liability for the Use of Artificial Intelligence in Indonesia*, Jurnal Info Sains: Informatika dan Sains, Vol.13, No.3 (2023).

bukan pada konstruksi pertanggungjawaban pidana atas penyalahgunaan AI. Baik Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana maupun Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik belum mengatur secara eksplisit mengenai AI-assisted crime, algorithmic fraud, maupun AI-generated deception. Kondisi ini menunjukkan adanya kekosongan hukum (*legal vacuum*) dalam hukum pidana Indonesia terkait kriminalitas berbasis AI.

Selain kesenjangan teoritis, terdapat pula *regulatory gap* dalam hukum positif Indonesia. Meskipun Indonesia telah memiliki sejumlah instrumen hukum yang relevan terhadap kejahatan digital, seperti Undang-Undang Informasi dan Transaksi Elektronik dan ketentuan pidana dalam Kitab Undang-Undang Hukum Pidana, regulasi tersebut pada dasarnya disusun untuk merespons cybercrime konvensional, bukan AI-assisted crime yang melibatkan pengambilan keputusan algoritmik dan sistem adaptif berbasis machine learning. Ketidadaan norma eksplisit mengenai *AI-generated deception*, *algorithmic fraud* dan atribusi kesalahan korporasi menunjukkan bahwa kerangka hukum pidana nasional belum sepenuhnya siap menghadapi evolusi kriminalitas ekonomi digital.¹²

Keterbatasan regulasi tersebut juga mencerminkan practical gap dalam penegakan hukum. Aparat penegak hukum menghadapi kesulitan dalam pembuktian digital, penelusuran sumber kesalahan algoritmik, serta penentuan standar pembuktian terhadap keputusan yang dihasilkan melalui sistem black-box. Persoalan ini tidak sekadar bersifat teknis, melainkan menyentuh fondasi hukum pidana modern mengenai relasi antara perbuatan, kesalahan dan pertanggungjawaban. Ketika causal chain tersembunyi dalam model AI yang tidak sepenuhnya dapat dijelaskan (*non-explainable systems*), mekanisme pembuktian konvensional menjadi kurang memadai.¹³

¹² Dosni Ana Ragita Pakpahan dan Anis Widyawati, *Reformulation of Cybercrime Regulations in The Misuse of Artificial Intelligence in Indonesia*, Law Research Review Quarterly, Vol.12, No.1 (2026).

¹³ Tri Suyud Nusantara dan Aloysius Wisnubroto, *Criminal Law Challenges and Solutions in Artificial Intelligence-Based Crime Prevention in Indonesia*, Multidisciplinary Indonesian Center Journal, Vol.3, No.1 (2026).

Kebaruan utama penelitian ini terletak pada perumusan konsep liability for algorithmic governance failure sebagai model rekonstruksi pertanggungjawaban pidana korporasi dalam AI-assisted business crime di Indonesia. Artikel ini berangkat dari premis bahwa perkembangan AI telah mentransformasi kejahatan bisnis dari pola kriminal konvensional menjadi bentuk kriminalitas korporasi yang bersifat prediktif, adaptif dan semakin sulit diatribusikan secara hukum. Penelitian ini mengisi *research gap* tersebut dengan menghubungkan studi tentang *AI governance*, *business crime* dan teori pertanggungjawaban pidana korporasi dalam satu kerangka analitis yang terintegrasi. Melalui pendekatan hukum normatif yang diperkuat analisis konseptual dan komparatif, artikel ini berupaya membangun model rekonstruksi regulasi hukum pidana Indonesia untuk merespons AI-assisted business crime secara lebih adaptif. Fokus utama penelitian diarahkan pada penggunaan *Corporate Criminal Liability Theory* sebagai landasan teoritis untuk menjelaskan atribusi kesalahan pidana terhadap korporasi ketika AI berperan sebagai instrumen atau medium kejahatan bisnis.

Berdasarkan latar belakang tersebut, penelitian ini difokuskan pada tiga persoalan utama. Pertama, bagaimana bentuk dan karakteristik Artificial Intelligence-assisted business crime dalam ekosistem ekonomi digital modern? Pertanyaan ini penting karena perkembangan AI tidak hanya mengubah modus operandi kejahatan bisnis, tetapi juga memperluas spektrum risiko kriminal melalui otomatisasi, prediksi perilaku dan pengambilan keputusan berbasis algoritma. Kedua, bagaimana pengaturan hukum pidana Indonesia merespons perkembangan AI-assisted business crime dan di mana letak kelemahan normatifnya? Persoalan ini berkaitan dengan kemampuan hukum positif Indonesia dalam mengantisipasi bentuk kriminalitas ekonomi yang tidak lagi sepenuhnya dilakukan oleh manusia secara langsung, melainkan melalui sistem teknologi semi-otonom. Ketiga, bagaimana *Corporate Criminal Liability Theory* dapat digunakan untuk merekonstruksi model pertanggungjawaban pidana terhadap korporasi yang menggunakan AI dalam aktivitas bisnis yang melanggar hukum? Fokus ini diarahkan untuk menjawab persoalan atribusi kesalahan pidana ketika AI menjadi instrumen utama dalam proses terjadinya tindak pidana.

Berdasarkan uraian rumusan masalah diatas, penelitian ini bertujuan untuk menganalisis bentuk dan karakteristik AI-assisted business crime dalam ekosistem ekonomi digital, mengevaluasi kelemahan regulasi hukum pidana Indonesia dalam merespons kriminalitas berbasis AI, serta merumuskan model rekonstruksi pertanggungjawaban pidana korporasi yang lebih adaptif melalui pendekatan *algorithmic governance failure* sebagai basis reformasi hukum pidana di Indonesia.

B. PEMBAHASAN

1. Transformasi *Business Crime* pada Era *Artificial Intelligence*

Kejahatan bisnis secara historis selalu berevolusi mengikuti perubahan struktur ekonomi dan perkembangan teknologi.¹⁴ Pada fase ekonomi industri, business crime umumnya berbentuk manipulasi akuntansi, penggelapan aset, kartel perdagangan, insider trading, atau praktik korupsi korporasi yang bertumpu pada interaksi manusia secara langsung.¹⁵ Karakter utama kejahatan pada periode ini adalah tingginya ketergantungan pada aktor individual yang memiliki akses terhadap informasi strategis atau otoritas pengambilan keputusan.¹⁶ Dengan kata lain, tindakan kriminal lahir melalui kontrol manusia yang relatif jelas sehingga identifikasi pelaku dan atribusi kesalahan pidana dapat dilakukan secara lebih linear.

Transformasi mulai terjadi seiring digitalisasi ekonomi global. Integrasi internet, komputasi awan, *big data* dan sistem transaksi elektronik mendorong pergeseran dari business crime konvensional menuju *digital business crime*.¹⁷ Pada tahap ini, kejahatan bisnis tidak lagi bergantung sepenuhnya pada dokumen fisik atau interaksi tatap muka, melainkan memanfaatkan infrastruktur digital untuk manipulasi data transaksi,

¹⁴ Sethard Fisher, *Economic Development and Crime: The Two May Be Associated as an Adaptation to Industrialism in Social Revolution*, The American Journal of Economics and Sociology, Vol.46, No.1 (1987).

¹⁵ Mark Lokanan, *Ai-Driven Detection of Industry-Specific Financial Fraud: A Theory-Informed NLP Approach*, Journal of White Collar and Corporate Crime, Vol.0, No.0 (2026).

¹⁶ Hartmut Berghoff dan Uwe Spiekermann, *Shady Business: On the History of White-Collar Crime*, Business History, Vol.60, No.3 (2018).

¹⁷ Rosita Eberechukwu Daraojimba, dkk., *Forensic Accounting in the Digital Age: A U.S. Perspective: Scrutinizing Methods and Challenges in Digital Financial Fraud Prevention*, Finance & Accounting Research Journal, Vol.5, No.11 (2023).

melakukan fraud, pencurian identitas dan rekayasa finansial lintas yurisdiksi. Perubahan tersebut meningkatkan skala dan kecepatan kejahatan, tetapi struktur kausalnya masih relatif dapat ditelusuri karena sistem digital pada dasarnya tetap beroperasi berdasarkan instruksi eksplisit manusia.

Perubahan yang jauh lebih fundamental muncul ketika Artificial Intelligence mulai diintegrasikan ke dalam aktivitas bisnis. AI tidak hanya mempercepat proses bisnis, tetapi juga mengubah logika pengambilan keputusan ekonomi melalui analisis prediktif, pembelajaran adaptif dan otomatisasi kompleks. Pada titik ini, business crime memasuki fase baru yang dapat disebut sebagai *AI-assisted business crime*, yaitu kejahatan bisnis yang sebagian atau seluruh operasionalisasinya bergantung pada sistem AI sebagai medium, akselerator, atau *decision engine*.¹⁸ Peralihan ini menandai perubahan paradigma: kriminalitas bisnis tidak lagi hanya berbicara tentang penyalahgunaan teknologi, melainkan tentang kriminalitas yang lahir dari sistem teknologi yang mampu “belajar” dan menyesuaikan perilaku secara dinamis.

Perbedaan antara *digital business crime* dan *AI-assisted business crime* bukan sekadar persoalan tingkat kecanggihan teknologi, melainkan perbedaan struktur kriminalitas. Dalam digital business crime, teknologi umumnya bersifat instrumen pasif. Sistem digital menjalankan instruksi yang dirancang manusia tanpa kapasitas adaptasi independen. Sebaliknya, dalam *AI-assisted business crime*, sistem dapat menghasilkan pola keputusan baru berdasarkan data yang terus berkembang. Implikasinya sangat signifikan: output yang merugikan dapat muncul tanpa adanya instruksi eksplisit yang secara langsung memerintahkan tindakan ilegal. Hal ini menciptakan tantangan besar bagi hukum pidana karena relasi antara tindakan, niat dan akibat tidak lagi sepenuhnya linear.¹⁹

¹⁸ Arif Mahmud, *Application and Criminalization of the Artificial Intelligence in Business: Recommendation to Counter the Regulatory Challenges*, Journal of Applied Security Research, Vol.18, No.4 (2023).

¹⁹ Sadia Sattar, *The Next Frontier of Cybercrime Law for Artificial Intelligence and Criminal Liability*, International Journal of Law and Policy, Vol.3, No.8 (2025).

Salah satu karakteristik utama AI-assisted business crime adalah *automation at scale*. Kejahatan yang sebelumnya membutuhkan intervensi manual kini dapat dijalankan secara otomatis dalam volume masif dan dalam waktu yang sangat singkat. Sebagai contoh, sistem AI dapat digunakan untuk menjalankan ribuan skenario penipuan investasi secara simultan dengan menyesuaikan narasi manipulatif berdasarkan profil psikologis target. Otomatisasi ini meningkatkan efisiensi kriminal secara drastis dan menurunkan biaya operasional pelaku. Dalam perspektif kriminologi ekonomi, fenomena ini menggeser cost-benefit calculation kriminal karena AI memperbesar potensi keuntungan dengan menekan biaya eksekusi.²⁰

Karakteristik kedua adalah *adaptive deception*. AI memungkinkan pelaku kejahatan mengembangkan mekanisme manipulasi yang jauh lebih persuasif dibanding penipuan digital konvensional. Sistem berbasis machine learning mampu menganalisis perilaku pengguna, pola transaksi, respons emosional, hingga preferensi konsumsi untuk menghasilkan strategi penipuan yang sangat personal. Di sinilah terjadi transformasi penting: fraud tidak lagi mengandalkan skema generik, melainkan berkembang menjadi deception yang bersifat prediktif dan individual. Tingkat sofistikasi ini membuat deteksi dini oleh korban maupun institusi keuangan menjadi jauh lebih sulit.²¹

Karakteristik ketiga adalah *anonymity through algorithmic opacity*. Banyak model AI, terutama yang berbasis *deep learning*, beroperasi sebagai *black-box systems* di mana logika internal pengambilan keputusan tidak sepenuhnya dapat dijelaskan. Kondisi ini memperumit proses atribusi kesalahan. Dalam business crime tradisional, penyidik dapat menelusuri rantai keputusan melalui dokumen, komunikasi internal, atau instruksi manajerial. Pada AI-assisted crime, rantai kausal sering tersembunyi dalam parameter model, training data dan interaksi algoritmik yang kompleks. Akibatnya, pembuktian hubungan antara aktor korporasi dan output kriminal menjadi jauh lebih menantang.

²⁰ M. Caldwell, dkk., *AI-Enabled Future Crime*, Crime Science, Vol.9, No.1 (2020).

²¹ Paolo Bailo, dkk., *A Review of Crime at Machine Speed: Criminological Aspects of Artificial Intelligence's Industrialisation of Deception*, Sci, Vol.8, No.3 (2026).

Karakteristik keempat adalah *distributed causation*. AI-assisted business crime jarang merupakan hasil tindakan tunggal. Kerugian ekonomi sering muncul dari interaksi kolektif antara desain model, kebijakan bisnis, kualitas data, konfigurasi sistem dan keputusan organisasi. Kondisi ini menantang fondasi hukum pidana yang cenderung mencari satu pelaku utama atau satu sumber kesalahan dominan. Dalam konteks AI, harm justru sering lahir dari akumulasi keputusan kecil yang secara individual tampak legal tetapi secara kolektif menghasilkan konsekuensi kriminal.

Transformasi tersebut memperlihatkan adanya *research gap* yang penting. Sebagian besar studi business crime masih beroperasi dalam kerangka fraud konvensional atau cybercrime generasi awal. Literatur AI, di sisi lain, lebih banyak menyoroti etika algoritma, bias data dan governance. Keterputusan kedua literatur ini menghasilkan blind spot akademik: belum banyak penelitian yang menjelaskan AI sebagai arsitek baru kriminalitas bisnis, khususnya dari perspektif hukum pidana korporasi.

Dari sudut regulasi, perubahan ini juga menyingkap *regulatory lag*. Hukum pidana umumnya bersifat reaktif karena merespons bentuk kriminal yang telah teridentifikasi secara sosial. Sementara itu, AI berkembang secara eksponensial dan menciptakan modus kriminal baru lebih cepat dibanding kemampuan legislasi untuk beradaptasi. Kesenjangan temporal ini sangat terlihat di Indonesia. Beberapa regulasi yang relevan, seperti Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 11 Tahun 2008 juncto Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, pada dasarnya masih dirancang untuk merespons kejahatan konvensional, cybercrime dan pelanggaran data.²² Di sisi lain, kebijakan seperti Strategi Nasional Kecerdasan Artifisial 2020–2045 dan Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial lebih berorientasi pada pengembangan dan etika AI,

²² Yang Meliana, *Dialektika Sistem Peradilan terhadap Analisis Kritis Perbandingan Litigasi Virtual dan Konvensional dalam Perspektif Hak Pembelaan Terdakwa*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.6, No.7 (2025).

bukan pengaturan pertanggungjawaban pidana. Akibatnya, Indonesia belum memiliki parameter normatif yang secara spesifik mengatur AI-assisted crime, algorithmic fraud, maupun atribusi kesalahan pidana korporasi atas penggunaan AI.²³

Dengan demikian, transformasi business crime pada era AI tidak dapat dipahami sebagai kelanjutan linear dari digital crime. AI telah merekonfigurasi struktur kejahatan bisnis pada level operasional, epistemologis dan normatif. Kejahatan bisnis kini bergerak menuju model kriminalitas yang otomatis, adaptif dan terdesentralisasi, sehingga menuntut perubahan cara pandang hukum pidana dalam memahami pelaku, kesalahan dan pertanggungjawaban. Transformasi inilah yang menjadi landasan untuk menganalisis bentuk-bentuk konkret AI-assisted business crime pada pembahasan berikutnya.

Manifestasi AI-assisted business crime menunjukkan bahwa kecerdasan buatan tidak beroperasi sebagai kategori kriminal yang tunggal, melainkan sebagai *crime multiplier* yang memperluas kapasitas pelaku dalam melakukan berbagai bentuk kejahatan ekonomi. AI dapat berfungsi sebagai instrumen manipulasi, alat prediksi, sistem otomatisasi, maupun medium penyamaran identitas. Keragaman fungsi ini menyebabkan AI-assisted business crime berkembang secara multidimensional, melintasi batas tradisional antara fraud, market abuse, financial deception dan pencucian aset. Oleh sebab itu, pemetaan tipologi kejahatan menjadi penting untuk memahami bagaimana AI mentransformasi praktik kriminal dalam sektor bisnis.

Bentuk-Bentuk *AI-Assisted Business Crime*:

a. *Algorithmic Fraud*

Salah satu bentuk paling signifikan dari AI-assisted business crime adalah *algorithmic fraud*, yaitu tindakan penipuan yang memanfaatkan algoritma AI untuk menghasilkan, memodifikasi, atau mengoptimalkan strategi penyesatan demi memperoleh keuntungan ekonomi ilegal.

²³ Muhammad Kautsar Ibrahim, dkk., *Urgensi Pembaruan Hukum dalam Menghadapi Kejahatan yang Melibatkan Teknologi Kecerdasan Buatan AI*, Journal of Legal, Political and Humanistic Inquiry, Vol.1, No.2 (2025).

Berbeda dari fraud konvensional yang bergantung pada intervensi manusia secara intensif, algorithmic fraud mengandalkan kemampuan AI untuk memproses data dalam volume besar dan menghasilkan respons manipulatif secara real-time.

Dalam praktik bisnis digital, algorithmic fraud dapat muncul melalui berbagai skema. Misalnya, AI digunakan untuk menganalisis perilaku konsumen sehingga sistem dapat mengidentifikasi individu dengan kerentanan tinggi terhadap investasi spekulatif. Berdasarkan data tersebut, algoritma kemudian menghasilkan penawaran yang dirancang secara personal untuk memaksimalkan probabilitas penipuan. Dengan pendekatan ini, fraud mengalami transformasi dari *mass deception* menuju *precision deception*.²⁴

Dari perspektif hukum pidana, algorithmic fraud menghadirkan persoalan serius terkait unsur kesengajaan. Pada fraud tradisional, niat menipu umumnya dapat ditelusuri melalui komunikasi, kontrak, atau representasi palsu yang dibuat pelaku. Dalam algorithmic fraud, representasi menyesatkan dapat dihasilkan oleh model AI yang terus mengoptimalkan strategi manipulatif tanpa instruksi eksplisit untuk menipu. Situasi ini menimbulkan pertanyaan kritis: apakah intensi kriminal dapat diatribusikan kepada operator, developer, atau korporasi yang mengimplementasikan algoritma tersebut?

b. Deepfake Financial Deception

Bentuk berikutnya adalah *deepfake financial deception*, yaitu penipuan finansial yang memanfaatkan media sintetis berbasis AI untuk memalsukan identitas visual maupun audio guna menciptakan ilusi autentisitas.²⁵ Fenomena ini menjadi salah satu perkembangan paling mengkhawatirkan dalam business crime modern karena menyerang fondasi utama transaksi bisnis, yaitu kepercayaan (*trust*). Dunia bisnis bertumpu pada asumsi bahwa identitas pihak yang berkomunikasi dapat

²⁴ Benjamin Zweers, dkk., *The AI-Fraud Diamond: A Novel Lens for Auditing Algorithmic Deception*, Artikel Ilmiah, arXiv, Ithaca, 2025.

²⁵ Pooja Kaushik, dkk., *Financial Fraud and Manipulation: The Malicious Use of Deepfakes in Business*, In *Advances in Business Information Systems and Analytics*, IGI Global Scientific Publishing, Hershey, 2025.

diverifikasi secara wajar. Deepfake merusak asumsi tersebut dengan memungkinkan pelaku mereplikasi suara CEO, CFO, komisaris, atau pihak berotoritas lainnya secara sangat meyakinkan.

Risiko kriminal dari deepfake jauh melampaui pemalsuan identitas konvensional. Teknologi AI memungkinkan rekayasa audio dan video dengan tingkat realisme tinggi sehingga verifikasi berbasis persepsi manusia menjadi semakin tidak dapat diandalkan. Dalam konteks bisnis, instruksi transfer dana, persetujuan investasi, atau otorisasi transaksi dapat dimanipulasi melalui simulasi identitas eksekutif perusahaan. Dari sudut pertanggungjawaban pidana, deepfake financial deception juga memunculkan persoalan *forensic complexity*. Pembuktian tidak hanya membutuhkan identifikasi pelaku, tetapi juga validasi keaslian bukti digital. Ketika batas antara autentik dan sintetis menjadi kabur, sistem pembuktian pidana menghadapi tantangan epistemologis yang serius.²⁶

c. AI-Driven Insider Trading dan Market Manipulation

AI juga membuka ruang baru bagi praktik *insider trading* dan manipulasi pasar yang jauh lebih canggih dibanding mekanisme tradisional. Dalam pasar modern yang sangat terdigitalisasi, kecepatan pengolahan informasi menjadi sumber keunggulan kompetitif. AI mampu menganalisis berita, sentimen pasar, data transaksi, bahkan perilaku investor dalam hitungan milidetik untuk menghasilkan keputusan perdagangan otomatis.

Permasalahan hukum muncul ketika AI digunakan untuk mengeksploitasi informasi material nonpublik atau menciptakan pola transaksi manipulatif yang memengaruhi harga pasar secara artifisial. Tidak seperti market manipulation konvensional yang sering dilakukan melalui transaksi eksplisit, manipulasi berbasis AI dapat disamarkan dalam volume perdagangan tinggi yang tampak normal secara statistik. AI bahkan dapat mengembangkan strategi *spoofing* dan *layering* secara adaptif membuat order besar guna menciptakan ilusi permintaan pasar,

²⁶ Bhaskardeep Khaund, *AI and Identity Security: The Threat of Deepfakes and the Future of Authentication*, World Journal of Advanced Engineering Technology and Sciences, Vol.15, No.3 (2025).

lalu membatalkannya setelah harga bergerak sesuai kepentingan pelaku. Karena perilaku ini dapat dijalankan otomatis dan dalam frekuensi tinggi, deteksi oleh regulator menjadi semakin kompleks. Masalah utama dari perspektif hukum pidana adalah kesulitan membedakan antara *legitimate algorithmic trading* dan *criminal algorithmic manipulation*. Ambiguitas ini menciptakan *regulatory gap*, terutama di yurisdiksi yang belum memiliki parameter jelas mengenai batas legal penggunaan AI dalam pasar keuangan.²⁷

d. *Synthetic Identity Fraud*

Perkembangan AI juga mempercepat munculnya *synthetic identity fraud*, yakni penciptaan identitas artifisial yang menggabungkan data nyata dan data palsu untuk membangun persona digital yang tampak kredibel.²⁸ Identitas sintetis dapat digunakan untuk membuka rekening, memperoleh pinjaman, membuat akun bisnis, atau melakukan transaksi bernilai tinggi tanpa mudah terlacak. Karakter unik *synthetic identity fraud* terletak pada sifatnya yang hibrid. Pelaku tidak sepenuhnya menggunakan identitas palsu, tetapi mencampurkan elemen autentik dengan data hasil rekayasa AI. Hal ini membuat mekanisme verifikasi identitas konvensional menjadi tidak efektif. Dalam ekosistem bisnis digital, kejahatan ini memiliki implikasi besar terhadap sektor perbankan, fintech, asuransi dan layanan kredit.²⁹ Risiko kerugian tidak hanya bersifat finansial, tetapi juga sistemik karena *synthetic identity fraud* dapat digunakan sebagai fondasi bagi kejahatan lanjutan, termasuk money laundering dan tax evasion.

e. *AI-Assisted Money Laundering*

Bentuk lain yang semakin memperoleh perhatian adalah *AI-assisted money laundering*, yakni penggunaan AI untuk menyamarkan asal-usul dana ilegal melalui pola transaksi yang kompleks dan adaptif.

²⁷ Anna Blachnio-Parzych dan Luigi Cornacchia, *Legal Protection against Financial Market Abuse: International and Local Perspectives*, Routledge, London, 2026.

²⁸ Rajesh Kumar Chakrawarti, dkk., *Cognitive Cyber Crimes in the Era of Artificial Intelligence*, Scrivener Publishing LLC, Beverly, 2026.

²⁹ Ravi Kiran Alluri, *Detecting Synthetic Identity Fraud Via Multimodal Customer Data Integration*, Journal of Artificial Intelligence & Cloud Computing, Vol.1, No.1 (2022).

Dalam pencucian uang tradisional, pelaku biasanya mengandalkan layering melalui transfer bertingkat, penggunaan rekening pihak ketiga, atau struktur perusahaan cangkang.³⁰ AI mengubah praktik tersebut dengan memungkinkan simulasi ribuan skenario transaksi untuk mengidentifikasi jalur pencucian yang paling sulit dideteksi sistem kepatuhan keuangan.

AI juga dapat digunakan untuk mempelajari pola deteksi yang digunakan institusi keuangan sehingga transaksi dapat dioptimalkan agar tetap berada di bawah threshold pengawasan. Dengan demikian, AI tidak sekadar membantu pencucian uang, tetapi secara aktif beradaptasi terhadap mekanisme anti-money laundering yang berlaku.³¹ Fenomena ini memperlihatkan *practical gap* yang serius. Rezim anti-pencucian uang modern sangat bergantung pada pattern detection dan anomaly detection. Ironisnya, AI kini juga memungkinkan pelaku memahami serta menghindari pola deteksi tersebut, sehingga tercipta perlombaan teknologi antara regulator dan pelaku kriminal.

Analisis terhadap berbagai bentuk AI-assisted business crime menunjukkan bahwa kejahatan bisnis berbasis AI memiliki karakter yang berbeda dari business crime konvensional. Kejahatan tidak lagi semata bergantung pada niat jahat individual, tetapi sering muncul melalui interaksi kompleks antara algoritma, data, model bisnis dan tata kelola korporasi. Temuan ini memperkuat argumen bahwa pendekatan hukum pidana yang terlalu berorientasi pada individual wrongdoing menjadi semakin tidak memadai. Oleh karena itu, pembahasan selanjutnya perlu diarahkan pada evaluasi terhadap kelemahan regulasi hukum pidana Indonesia dalam merespons transformasi kriminalitas bisnis berbasis AI.

³⁰ Halim Hermanto dan Lolita Fitriyana, *Pengaturan Penyitaan Aset Kripto sebagai Hasil Tindak Pidana Pencucian Uang di Indonesia*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.6, No.7 (2025).

³¹ Richard John Lowe, *Anti-Money Laundering – The Need for Intelligence*, Journal of Financial Crime, Vol.24, No.3 (2017).

2. Kelemahan Regulasi Hukum Pidana Indonesia dalam Merespons *AI-Assisted Business Crime*

Perkembangan *AI-assisted business crime* memperlihatkan ketegangan yang semakin tajam antara percepatan inovasi teknologi dan kapasitas adaptasi hukum pidana.³² Ketegangan ini menjadi sangat nyata di Indonesia, di mana perkembangan teknologi digital bergerak secara eksponensial, sementara reformasi regulasi pidana cenderung berlangsung secara gradual dan reaktif. Problem utamanya bukan semata ketiadaan aturan mengenai kejahatan digital, melainkan ketidakmampuan kerangka hukum yang ada untuk menangkap karakter kriminalitas yang lahir dari sistem algoritmik adaptif.³³ Dengan kata lain, tantangan regulatif *AI-assisted business crime* bukan sekadar soal legal vacuum, tetapi juga menyangkut *conceptual inadequacy* dalam konstruksi hukum pidana nasional.

Secara normatif, Indonesia memang telah memiliki sejumlah instrumen hukum yang dapat digunakan untuk merespons kejahatan digital dan kejahatan bisnis, termasuk Kitab Undang-Undang Hukum Pidana, Undang-Undang Informasi dan Transaksi Elektronik, regulasi perlindungan data pribadi, serta berbagai aturan sektoral di bidang jasa keuangan dan perdagangan elektronik. Pada level tekstual, instrumen tersebut tampak menyediakan landasan hukum yang cukup luas untuk menjerat tindakan penipuan, manipulasi data, akses ilegal, maupun kerugian ekonomi berbasis sistem elektronik.³⁴ Namun, ketika norma-norma tersebut diuji terhadap *AI-assisted business crime*, muncul keterbatasan mendasar yang menunjukkan bahwa keberadaan regulasi tidak selalu identik dengan kecukupan regulatif.

Untuk menilai kecukupan regulasi tersebut, terlebih dahulu perlu dipetakan instrumen hukum yang saat ini berkaitan dengan AI di Indonesia.

³² Dian Juniarso, dkk., *Reformasi Kebijakan Pidana Nasional terhadap Kejahatan Siber Berbasis AI melalui Pendekatan Hukum Progresif*, Jurnal Impresi Indonesia, Vol.5, No.1 (2026).

³³ Riska Fitriya, dkk., *Melacak Jejak Pidana AI: Status Subjek Hukum dan Model Pertanggungjawaban di Indonesia*, As-Syar'i: Jurnal Bimbingan & Konseling Keluarga, Vol.8, No.1 (2026).

³⁴ Muhammad Gustryani dan Zainal Arifin Hoesein, *Peran Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi dalam Perlindungan Data dan Privasi di Era Ekonomi Digital*, Jurnal Minfo Polgan, Vol.14, No.2 (2025).

Hingga saat ini, Indonesia belum memiliki undang-undang khusus yang secara komprehensif mengatur Artificial Intelligence. Pengaturan yang tersedia masih tersebar dalam berbagai instrumen sektoral.³⁵ Pertama, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana menyediakan dasar umum mengenai tindak pidana penipuan, pemalsuan dan kejahatan ekonomi, namun seluruh konstruksi pertanggungjawabannya masih berorientasi pada pelaku manusia maupun korporasi dalam pengertian konvensional. Kedua, Undang-Undang Nomor 11 Tahun 2008 juncto Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik mengatur akses ilegal, manipulasi informasi elektronik dan gangguan sistem elektronik, tapi belum menjangkau kejahatan yang timbul dari autonomous algorithmic decision-making.³⁶

Ketiga, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi lebih berfokus pada lawful processing, persetujuan subjek data dan perlindungan privasi, sehingga belum mengatur atribusi pertanggungjawaban pidana atas penyalahgunaan AI. Keempat, Strategi Nasional Kecerdasan Artifisial 2020-2045 serta Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial hanya berfungsi sebagai kerangka kebijakan dan pedoman etik, bukan sebagai norma pidana yang mengikat. Dengan demikian, pengaturan AI di Indonesia saat ini masih bersifat parsial, sektoral dan dominan soft-law.³⁷

Adapun salah satu kelemahan paling mendasar terletak pada fakta bahwa hukum pidana Indonesia masih beroperasi dalam paradigma *human-centric criminal liability*.³⁸ Struktur pertanggungjawaban pidana dibangun di atas asumsi klasik bahwa tindak pidana selalu merupakan hasil tindakan sadar manusia atau entitas hukum yang bertindak melalui manusia.

³⁵ Nasman, dkk., *Etika dan Pertanggungjawaban Penggunaan Artificial Intelligence di Indonesia*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.5, No.10 (2024).

³⁶ Saiful Hamdi, dkk., *Implikasi Hukum Penggunaan Artificial Intelligence sebagai Bewijsmiddelen dalam Penegakan Hukum di Indonesia (Telaah Pragmatisme Abduksi)*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.4, No.10 (2023).

³⁷ Shabrina Fadiah Ghazmi, *Urgensi Pengaturan Artificial Intelligence pada Sektor Bisnis Daring di Indonesia*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.2, No.8 (2021).

³⁸ Hendri Khuan, *Void in Law: Criminal Regulation Vacuum on the Detrimental Impact of AI Artificial Intelligence*, Journal of Strafvordering Indonesian, Vol.2, No.3 (2025).

Paradigma ini bekerja cukup efektif untuk kejahatan konvensional maupun cybercrime generasi awal. Akan tetapi, AI-assisted business crime memperkenalkan bentuk kausalitas yang jauh lebih kompleks karena keputusan yang menimbulkan kerugian dapat lahir dari interaksi antara manusia, korporasi, data dan algoritma yang terus berevolusi.

Persoalan tersebut mengungkap *regulatory gap* pertama, yakni kekosongan norma terkait *AI-specific criminal conduct*. Hingga saat ini, hukum positif Indonesia belum menyediakan kategori normatif yang secara eksplisit mengatur kejahatan yang melibatkan keputusan algoritmik semi-otonom. Absennya norma khusus bukan hanya persoalan terminologi. Ketiadaan pengakuan terhadap AI sebagai faktor hukum yang relevan menyebabkan aparat penegak hukum cenderung memaksakan konstruksi lama terhadap fenomena baru. Akibatnya, penegakan hukum berisiko bersifat reduksionis karena kompleksitas AI direduksi menjadi sekadar alat elektronik biasa.

Kelemahan kedua terletak pada ketidakjelasan subjek pertanggungjawaban pidana. Dalam *AI-assisted business crime*, rantai aktor yang terlibat sering kali bersifat multilapis: developer membangun model, vendor menyediakan infrastruktur, operator mengimplementasikan sistem, manajemen menentukan parameter bisnis dan korporasi memperoleh manfaat ekonomi.³⁹ Struktur semacam ini menimbulkan persoalan atribusi yang tidak sederhana. Hukum pidana Indonesia belum memiliki parameter normatif yang jelas untuk menentukan pada titik mana kegagalan algoritmik berubah menjadi kesalahan pidana korporasi. Akibatnya, ruang interpretasi menjadi terlalu luas dan berpotensi menimbulkan inkonsistensi penegakan hukum. Problem ini semakin serius karena AI menantang doktrin klasik mengenai unsur kesalahan. Dalam hukum pidana, legitimasi pemidanaan sangat bergantung pada kemampuan untuk membuktikan adanya *mens rea* atau bentuk culpability tertentu.

³⁹ Iman Nurjaman dan Yuyut Prayuti, *Celah Regulasi Penegakan Hukum dalam Mengatasi Pencucian Uang dari Kejahatan Ekonomi melalui Aset Digital di Indonesia*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.6, No.7 (2025).

AI-assisted crime mengganggu struktur pembuktian tersebut. Kerugian ekonomi yang signifikan dapat timbul tanpa adanya perintah eksplisit untuk melanggar hukum. Dalam banyak kasus, harm justru muncul dari kombinasi model machine learning yang bias, absennya audit internal dan target bisnis agresif. Masalahnya, hukum pidana Indonesia belum mengembangkan parameter yang memadai untuk menilai *algorithmic negligence* atau *governance failure* sebagai bentuk kesalahan pidana.

Kelemahan ketiga adalah absennya standar due diligence dalam tata kelola AI korporasi. Dalam banyak yurisdiksi maju, diskursus regulasi AI mulai bergeser dari sekadar pelarangan menuju *governance-based compliance*.⁴⁰ Korporasi didorong untuk melakukan risk assessment, impact assessment, audit algoritma dan mekanisme explainability sebelum AI diimplementasikan dalam sektor berisiko tinggi. Indonesia belum memiliki kerangka kewajiban serupa yang terintegrasi dengan rezim pertanggungjawaban pidana. Akibatnya, hukum pidana nasional cenderung bekerja setelah kerugian terjadi, bukan sebagai instrumen pencegahan berbasis pengelolaan risiko.

Keterbatasan ini menunjukkan adanya *practical gap* dalam pendekatan penal Indonesia. Sistem hukum pidana nasional masih sangat menekankan pendekatan represif berbasis pelanggaran yang telah selesai terjadi (*ex post enforcement*). Padahal, AI-assisted business crime menuntut model regulasi yang lebih proaktif dan prediktif. Menunggu terjadinya kerugian besar sebelum intervensi hukum dilakukan jelas tidak sejalan dengan karakter AI yang mampu menghasilkan harm dalam skala massif dalam waktu singkat.

Kelemahan keempat menyangkut problematika pembuktian digital berbasis black-box systems. Salah satu tantangan terbesar AI modern adalah opacity atau tertutupan logika internal sistem. Fenomena *black-box algorithm* mengacu pada kondisi ketika input dan output dapat diamati,

⁴⁰ Daniel Weimer, dkk., *Scaling of End-To-End Governance Risk Assessments for AI Systems (Practitioner Track)*, Prosiding Symposium on Scaling AI Assessments (2024).

tetapi proses internal pembentukan keputusan tidak sepenuhnya dapat dijelaskan.⁴¹ Dalam konteks pidana, kondisi ini menimbulkan implikasi serius terhadap pembuktian kausalitas. Penyidik mungkin dapat membuktikan bahwa suatu output AI menyebabkan kerugian, tetapi belum tentu mampu menjelaskan bagaimana keputusan tersebut terbentuk atau siapa yang secara hukum harus menanggung akibatnya.

Masalah pembuktian ini tidak bersifat teknis semata; ia menyentuh legitimasi proses peradilan pidana. Sistem peradilan pidana mensyaratkan pembuktian yang dapat diuji melalui proses adversarial dan rasional. Jika output AI tidak dapat dijelaskan secara memadai, maka standar pembuktian konvensional menghadapi krisis epistemik. Hal ini memperlihatkan *theoretical gap* yang serius antara perkembangan teknologi komputasional dan struktur evidentiary law yang berlaku.

Kelemahan kelima berkaitan dengan fragmentasi regulasi sektoral. Regulasi yang berkaitan dengan teknologi digital, perlindungan data, keuangan, persaingan usaha dan perlindungan konsumen di Indonesia berkembang dalam rezim yang relatif terpisah.⁴² Fragmentasi ini menyulitkan pembentukan respons hukum yang komprehensif terhadap AI-assisted business crime karena risiko kriminal AI hampir selalu bersifat lintas sektor. Satu bentuk kejahatan dapat sekaligus melibatkan pelanggaran data, fraud keuangan, manipulasi pasar dan penyalahgunaan sistem elektronik. Tanpa harmonisasi regulatif, respons hukum cenderung parsial dan kurang efektif.

Dari analisis tersebut terlihat bahwa kelemahan regulasi hukum pidana Indonesia tidak hanya terletak pada ketiadaan aturan khusus mengenai AI. Persoalan yang lebih mendasar adalah adanya ketidaksesuaian struktural antara paradigma hukum pidana konvensional dan karakter AI-assisted business crime yang adaptif, non-linear dan berbasis distribusi keputusan.

⁴¹ Uwe Peters, *Explainable AI Lacks Regulative Reasons: Why AI and Human Decision-Making Are Not Equally Opaque*, AI and Ethics, Vol.3, No.3 (2023).

⁴² Saifullah, dkk., *The Evaluation of The Indonesian Fintech Law from The Perspective of Regulatory Technology Paradigms to Mitigate Illegal Fintech*, Jurisdictie: Jurnal Hukum dan Syariah, Vol.14, No.2 (2024).

Hukum pidana Indonesia pada dasarnya masih dirancang untuk merespons kejahatan dengan pelaku yang dapat diidentifikasi secara langsung, rantai kausal yang relatif jelas dan bentuk kesalahan yang dapat ditelusuri melalui niat individual. Ketiga asumsi tersebut semakin sulit dipertahankan dalam konteks kriminalitas bisnis berbasis AI.

Dalam perspektif *ius constituendum*, hukum pidana Indonesia idealnya tidak hanya menambahkan AI sebagai terminologi baru dalam regulasi yang telah ada, melainkan membangun kerangka hukum khusus yang mampu mengakomodasi karakter AI-assisted crime. Setidaknya terdapat tiga elemen yang perlu diakomodasi. Pertama, perumusan norma pidana yang secara eksplisit mengakui AI-assisted criminal conduct, termasuk algorithmic fraud, AI-generated deception dan autonomous market manipulation. Kedua, pengembangan parameter pertanggungjawaban pidana korporasi berbasis algorithmic accountability untuk menentukan batas tanggung jawab developer, operator dan korporasi pengguna. Ketiga, pembentukan kewajiban hukum berupa mandatory AI governance yang mencakup risk assessment, algorithmic audit, explainability dan human oversight. Model regulasi semacam ini akan memperkuat fungsi preventif hukum pidana sekaligus memberikan kepastian hukum dalam penanganan kejahatan bisnis berbasis AI.

Temuan ini mengarah pada satu implikasi penting. Reformasi regulasi pidana Indonesia tidak dapat berhenti pada penambahan norma larangan baru. Yang diperlukan adalah rekonstruksi lebih mendasar terhadap model pertanggungjawaban pidana itu sendiri, khususnya terkait bagaimana kesalahan korporasi dibangun ketika AI menjadi bagian dari proses pengambilan keputusan bisnis. Atas dasar itulah pembahasan selanjutnya akan menganalisis AI-assisted business crime melalui perspektif *Corporate Criminal Liability Theory* untuk merumuskan model pertanggungjawaban yang lebih adaptif terhadap realitas ekonomi digital.

3. Analisis *AI-Assisted Business Crime* melalui *Corporate Criminal Liability Theory*

Diskursus mengenai AI-assisted business crime pada akhirnya bermuara pada satu pertanyaan fundamental dalam hukum pidana: siapakah subjek yang secara sah dapat dimintai pertanggungjawaban ketika kerugian ekonomi timbul dari keputusan yang dihasilkan atau dipengaruhi oleh sistem AI? Pertanyaan ini tampak sederhana, namun secara doktrinal menyentuh inti legitimasi pemidanaan.⁴³ Hukum pidana tidak hanya menuntut adanya perbuatan melawan hukum, tetapi juga mensyaratkan adanya subjek yang memiliki kapasitas untuk memikul kesalahan. Kompleksitas muncul ketika AI menempati posisi ambigu bukan manusia, bukan badan hukum, namun memiliki kapasitas operasional yang secara faktual memengaruhi lahirnya akibat hukum.

Dalam kerangka hukum pidana klasik, problem pertanggungjawaban biasanya diselesaikan melalui hubungan langsung antara pelaku, perbuatan dan akibat. Struktur ini relatif stabil ketika tindak pidana dilakukan oleh individu atau bahkan korporasi dalam model bisnis konvensional. AI-assisted business crime merusak linearitas tersebut. Kerugian ekonomi tidak selalu lahir dari instruksi eksplisit, melainkan dapat muncul dari interaksi berlapis antara desain algoritma, parameter bisnis, kualitas data, tujuan komersial dan mekanisme pembelajaran mesin. Karena itu, pendekatan yang hanya berupaya menemukan satu aktor dominan sebagai pelaku utama menjadi semakin tidak memadai.

Pada titik inilah Corporate Criminal Liability memperoleh signifikansi analitis. Teori ini memungkinkan pergeseran fokus dari individual wrongdoing menuju organizational responsibility. Alih-alih bertanya siapa yang secara fisik menjalankan tindakan, analisis diarahkan pada siapa yang memiliki kontrol normatif, kapasitas pengawasan dan keuntungan ekonomi dari sistem yang menghasilkan harm. Dalam konteks AI-assisted business crime, entitas yang paling sering memenuhi ketiga unsur tersebut adalah korporasi.

⁴³ Yanel Garsione Damanik, *Problematisasi Pencegahan dan Kejahatan di Bidang Ekonomi*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.1, No.4 (2020).

Namun, penerapan Corporate Criminal Liability Theory terhadap AI-assisted crime tidak dapat dilakukan secara mekanis. Model klasik pertanggungjawaban pidana korporasi dibangun pada asumsi bahwa tindakan organisasi pada akhirnya tetap dapat direduksi ke tindakan manusia. AI menantang asumsi ini karena menghadirkan lapisan *algorithmic agency* yang memperumit relasi antara kehendak organisasi dan outcome operasional. Oleh sebab itu, analisis dalam penelitian ini menggunakan tiga skenario untuk menguji elastisitas teori tersebut.

a. Skenario Pertama: AI sebagai Instrumen Pasif

Skenario pertama menggambarkan kondisi ketika AI berfungsi sebagai alat bantu yang sepenuhnya dikendalikan manusia. Dalam model ini, AI tidak memiliki ruang otonomi substantif; sistem hanya mengeksekusi parameter yang secara jelas ditentukan oleh operator atau korporasi. Secara doktrinal, konstruksi ini paling dekat dengan penggunaan instrumen teknologi konvensional.

Dalam situasi seperti ini, pertanggungjawaban pidana relatif tidak menimbulkan problem teoretis yang serius. Jika korporasi secara sadar menggunakan AI untuk memanipulasi transaksi, menghasilkan laporan keuangan palsu, atau menjalankan penipuan investasi otomatis, maka AI tidak lebih dari alat kriminal yang memperbesar efisiensi kejahatan.⁴⁴ Unsur kesalahan dapat diatribusikan melalui *Identification Theory* maupun *Vicarious Liability*, karena kehendak kriminal masih dapat ditelusuri pada aktor manusia yang mengendalikan sistem.⁴⁵

Dari perspektif hukum pidana, AI pada skenario ini memiliki status analog dengan perangkat lunak biasa. Fokus analisis tetap berada pada niat pelaku manusia atau keputusan korporasi. Oleh karena itu, kerangka pertanggungjawaban klasik masih memadai. Problem regulasi pada tahap ini lebih berkaitan dengan penyesuaian instrumen pembuktian digital daripada perubahan radikal dalam doktrin kesalahan.

⁴⁴ Yang Meliana, *Urgensi Formulasi Perlindungan Hukum dan Kepastian Pidana terhadap Pengaturan Tindak Pidana Deepfake dalam Sistem Hukum Pidana Nasional*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.6, No.7 (2025).

⁴⁵ Mardian Putra Frans, dkk., *Pertanggungjawaban Pidana Bank sebagai Pengguna Artificial Intelligence*, Jurnal USM Law Review, Vol.7, No.2 (2024).

b. Skenario Kedua: *AI Semi-Otonom*

Kompleksitas meningkat secara signifikan ketika AI beroperasi secara semi-otonom. Pada model ini, manusia tetap mendesain arsitektur awal sistem, tetapi AI memperoleh kapasitas pembelajaran adaptif yang memungkinkan sistem menghasilkan keputusan baru berdasarkan data yang terus berkembang. Output operasional tidak lagi sepenuhnya identik dengan instruksi awal. Skenario ini menciptakan area abu-abu dalam pertanggungjawaban pidana. Korporasi mungkin tidak pernah memberikan instruksi eksplisit untuk melakukan pelanggaran, tetapi tetap memperoleh manfaat dari perilaku AI yang agresif atau manipulatif. Di sinilah konsep kesalahan berbasis intentional wrongdoing mulai kehilangan daya jelaskan.

Masalah utama bukan lagi adanya niat jahat yang eksplisit, melainkan apakah korporasi telah gagal memenuhi standar kehati-hatian yang seharusnya dijalankan dalam deployment AI. Pertanyaan normatifnya bergeser dari *Did the corporation intend the crime?* menuju *Should the corporation have reasonably foreseen and prevented the risk?*

Pergeseran ini sangat penting karena menunjukkan bahwa AI-assisted business crime pada level semi-otonom lebih tepat dianalisis melalui konsep *corporate negligence* atau *reckless governance*. Kesalahan korporasi tidak terletak semata pada tindakan aktif melakukan fraud, tetapi pada kegagalan membangun kontrol internal, audit risiko dan pengawasan terhadap sistem AI yang berpotensi menghasilkan harm.

Dalam konteks ini, *Aggregation Theory* menawarkan kerangka yang lebih relevan. Kesalahan tidak muncul dari satu individu, melainkan dari akumulasi kegagalan kolektif berbagai unit organisasi tim teknis, manajemen risiko, compliance dan direksi. AI-assisted harm pada skenario ini dengan demikian lebih tepat dibaca sebagai kegagalan tata kelola daripada deviasi personal.

c. Skenario Ketiga: *AI Highly Autonomous*

Skenario ketiga merepresentasikan bentuk paling kompleks dari AI-assisted business crime, yaitu ketika AI beroperasi dengan tingkat otonomi yang tinggi dan menghasilkan keputusan yang secara substantif tidak dapat diprediksi secara penuh oleh manusia. Pada tahap ini, sistem bukan hanya mengoptimalkan parameter yang ada, tetapi juga mengembangkan strategi baru melalui proses pembelajaran berkelanjutan.⁴⁶ Skenario ini menimbulkan disrupti paling besar terhadap doktrin pertanggungjawaban pidana klasik. Problem utamanya terletak pada melemahnya hubungan antara kontrol manusia dan output AI. Jika suatu sistem perdagangan berbasis AI mengembangkan pola manipulasi pasar yang tidak pernah dirancang secara eksplisit oleh developer maupun direksi, atribusi kesalahan menjadi sangat problematis.

Pada titik ini, Identification Theory menjadi semakin lemah karena tidak terdapat satu *directing mind* yang dapat dikatakan secara sadar menghendaki outcome kriminal. Bahkan Vicarious Liability juga mengalami keterbatasan karena tindakan AI tidak sepenuhnya identik dengan tindakan agen manusia.

Situasi tersebut mengungkap *theoretical gap* mendasar dalam *Corporate Criminal Liability Theory* klasik: teori ini belum sepenuhnya dirancang untuk menjelaskan criminality yang lahir dari autonomous computational systems. Namun, bukan berarti korporasi harus dibebaskan dari tanggung jawab. Sebaliknya, justru di level otonomi tinggi ini pendekatan pertanggungjawaban harus direorientasikan.

Penelitian ini berargumen pada *AI highly autonomous*, kesalahan pidana korporasi seharusnya tidak lagi dibangun berdasarkan pencarian niat individual, tetapi melalui evaluasi terhadap *algorithmic governance failure*. Pertanyaannya bukan siapa yang memerintahkan pelanggaran, melainkan apakah korporasi telah membangun sistem pengawasan yang memadai guna mengendalikan risiko kriminal dari AI yang dioperasikan.

⁴⁶ Ryan Abbott dan Alexander Sarch, *Punishing Artificial Intelligence: Legal Fiction or Science Fiction, In Legal Aspects of Autonomous Systems: A Comparative Approach*, Springer International Publishing, Berlin, 2024.

Argumentasi ini menghasilkan reinterpretasi penting terhadap Corporate Criminal Liability Theory. Pertanggungjawaban pidana korporasi tidak lagi cukup dipahami sebagai liability atas tindakan individu dalam organisasi (*liability for acts*). Dalam konteks AI, liability harus diperluas menjadi tanggung jawab atas kegagalan institusional dalam mengelola risiko algoritmik (*liability for governance failure*). Perubahan ini memiliki implikasi normatif yang signifikan. Jika kegagalan tata kelola algoritmik diakui sebagai basis culpability, maka fokus hukum pidana bergeser menuju penilaian atas kualitas governance korporasi. Parameter seperti AI risk assessment, explainability, audit trail, monitoring mechanism dan internal compliance tidak lagi sekadar instrumen manajemen risiko, tetapi dapat menjadi indikator hukum untuk menilai keberadaan kesalahan pidana.

Analisis tiga skenario tersebut menunjukkan bahwa AI telah mentransformasi struktur pertanggungjawaban pidana korporasi secara mendasar. Semakin tinggi tingkat otonomi AI, semakin lemah efektivitas model pertanggungjawaban klasik yang berorientasi pada individual intent. Sebaliknya, semakin kuat kebutuhan untuk mengembangkan model liability yang berbasis governance responsibility. Temuan ini menjadi kontribusi teoritis utama penelitian ini: Corporate Criminal Liability Theory tetap relevan dalam era AI, tetapi hanya apabila direkonstruksi dari paradigma kesalahan individual menuju paradigma kegagalan tata kelola algoritmik. Atas dasar itu, pembahasan berikutnya diarahkan pada perumusan model rekonstruksi regulasi hukum pidana Indonesia yang mampu mengakomodasi perubahan paradigma tersebut.

4. Rekonstruksi Regulasi Hukum Pidana Indonesia terhadap *AI-Assisted Business Crime*

Analisis sebelumnya menunjukkan bahwa problem utama AI-assisted business crime di Indonesia bukan semata-mata absennya norma yang secara eksplisit menyebut artificial intelligence. Persoalan yang lebih mendasar terletak pada ketidaksesuaian antara arsitektur hukum pidana konvensional dan karakter kriminalitas berbasis algoritma yang adaptif,

non-linear, serta beroperasi melalui distribusi keputusan organisasi. Kondisi ini menuntut rekonstruksi regulasi yang tidak berhenti pada penambahan norma prohibitif, melainkan menyentuh fondasi konseptual pertanggungjawaban pidana itu sendiri.

Rekonstruksi regulasi hukum pidana dalam konteks AI-assisted business crime setidaknya harus diarahkan pada tiga level: rekonstruksi subjek pertanggungjawaban, rekonstruksi basis culpability dan rekonstruksi mekanisme penegakan hukum. Ketiga level tersebut saling berkaitan karena kegagalan pada salah satu level akan menghasilkan respons hukum yang parsial dan kurang efektif. Reformasi yang hanya menambah larangan baru tanpa memperbaiki struktur pertanggungjawaban berpotensi menciptakan norma yang simbolik tetapi sulit diimplementasikan.

a. Rekonstruksi Subjek Pertanggungjawaban Pidana

Fondasi pertama yang perlu direformulasi adalah konstruksi mengenai subjek pertanggungjawaban pidana. Hukum pidana Indonesia secara tradisional mengenal manusia dan korporasi sebagai subjek hukum utama.⁴⁷ Struktur ini memadai ketika tindak pidana dilakukan melalui tindakan langsung manusia atau kebijakan organisasi yang dapat diidentifikasi secara jelas. AI-assisted business crime menghadirkan konfigurasi yang lebih kompleks karena keputusan operasional dapat terbentuk melalui interaksi antara developer, operator, vendor teknologi dan korporasi pengguna.

Sebelum merekonstruksi subjek pertanggungjawaban pidana, perlu ditegaskan terlebih dahulu posisi AI dalam perspektif hukum pidana. Secara teoritis, terdapat perdebatan mengenai kemungkinan pemberian legal personhood kepada artificial intelligence, terutama karena sistem AI modern mampu melakukan pembelajaran adaptif dan menghasilkan keputusan semi-otonom. Namun, dalam konteks hukum pidana Indonesia, AI belum dapat dikualifikasikan sebagai subjek hukum yang mandiri. Secara doktrinal, subjek hukum pidana masih terbatas pada manusia dan, dalam kondisi tertentu, korporasi sebagai entitas hukum.

⁴⁷ Yatini, dkk., *Reformulasi Konstruksi Pidana dalam Menjerat Pelaku Tindak Pidana Korporasi*, Jurnal Hukum dan Pembangunan Ekonomi, Vol.7, No.1 (2019).

AI pada dasarnya merupakan sistem komputasional yang beroperasi berdasarkan data, algoritma dan parameter yang dirancang oleh manusia. Meskipun AI dapat menghasilkan keputusan yang tampak otonom, sistem tersebut tidak memiliki kesadaran moral (*moral agency*), kehendak bebas (*free will*), maupun kapasitas untuk memahami larangan hukum sebagaimana disyaratkan dalam doktrin kesalahan pidana. Ketiadaan elemen-elemen tersebut menyebabkan AI belum memenuhi syarat fundamental untuk memikul pertanggungjawaban pidana secara langsung.

Dari perspektif kebijakan hukum pidana, pengakuan AI sebagai subjek pidana juga berpotensi menimbulkan moral hazard. Korporasi dapat menjadikan AI sebagai tameng pertanggungjawaban dengan mengalihkan kesalahan dari pengambil keputusan manusia kepada sistem algoritmik. Oleh karena itu, penelitian ini menolak pendekatan yang menempatkan AI sebagai pelaku tindak pidana mandiri. AI lebih tepat diposisikan sebagai objek regulasi, instrumen operasional, atau sumber risiko hukum yang menimbulkan pertanggungjawaban bagi manusia dan korporasi yang mendesain, mengoperasikan, atau memperoleh manfaat ekonomi dari penggunaannya.

Dalam konteks tersebut, rekonstruksi tidak harus mengarah pada pengakuan AI sebagai subjek pidana mandiri. Pendekatan tersebut justru berisiko menciptakan problem filosofis dan yuridis yang lebih besar karena AI tidak memiliki moral agency dalam pengertian hukum pidana klasik. Alternatif yang lebih realistis adalah memperluas spektrum subjek pertanggungjawaban melalui pendekatan *multi-layered accountability*, yakni model yang mengakui adanya tanggung jawab bertingkat berdasarkan derajat kontrol dan manfaat ekonomi terhadap sistem AI.

Dalam model ini, developer dapat dimintai pertanggungjawaban ketika desain sistem secara inheren menciptakan risiko kriminal yang dapat diperkirakan. Operator sendiri bertanggung jawab atas penggunaan sistem secara melawan hukum atau tanpa pengawasan memadai.

Korporasi sebagai beneficiary utama memikul tanggung jawab atas kegagalan tata kelola yang memungkinkan AI menghasilkan harm. Pendekatan multilapis ini lebih kompatibel dengan struktur distribusi risiko pada ekosistem AI modern.

b. Rekonstruksi Basis Culpability: Dari Intentional Fault menuju *Algorithmic Governance Failure*

Rekonstruksi kedua menyentuh aspek yang paling fundamental dalam hukum pidana, yakni basis kesalahan. Paradigma klasik menempatkan intentional wrongdoing sebagai pusat legitimasi pembedaan. Meskipun konsep kelalaian telah lama dikenal, praktik hukum pidana ekonomi masih sangat dipengaruhi oleh pencarian niat individual sebagai indikator utama culpability.⁴⁸

AI-assisted business crime menunjukkan bahwa pendekatan tersebut semakin tidak memadai. Banyak harm ekonomi tidak lahir dari niat eksplisit untuk melanggar hukum, tetapi dari kombinasi deployment AI berisiko tinggi, kegagalan audit, bias data dan absennya pengawasan organisasi. Dalam situasi demikian, pencarian *mens rea* individual semata justru dapat mengaburkan sumber kesalahan yang sebenarnya.

Penelitian ini mengusulkan pergeseran basis culpability dari *intent-centric liability* menuju *governance-centric liability*. Dalam model ini, kesalahan pidana korporasi dapat dibangun melalui pembuktian adanya *algorithmic governance failure*, yaitu kegagalan institusional untuk menjalankan kewajiban kehati-hatian dalam pengelolaan AI.

Konsep ini memiliki nilai normatif yang penting karena memperluas pemahaman mengenai kesalahan pidana tanpa menghilangkan prinsip culpability. Kesalahan tidak lagi semata dicari dalam niat jahat eksplisit, tetapi dalam kegagalan sistemik yang secara rasional dapat diperkirakan dan dicegah. Dengan demikian, hukum pidana tetap menjaga legitimasi moralnya sekaligus menjadi lebih responsif terhadap realitas teknologi modern.

⁴⁸ Marilyn D. McShane dan Frank P. Williams III, *The American Court System*, Routledge, London, 2020.

c. *AI Compliance Obligation* sebagai Kewajiban Hukum Korporasi

Rekonstruksi ketiga berkaitan dengan integrasi kewajiban kepatuhan AI ke dalam rezim hukum pidana korporasi. Dalam banyak sistem hukum modern, compliance tidak lagi dipandang sekadar mekanisme tata kelola internal, melainkan instrumen regulatif untuk mencegah terjadinya harm sebelum pelanggaran terjadi.⁴⁹ Indonesia memerlukan standar minimum kewajiban hukum bagi korporasi yang mengoperasikan AI dalam sektor berisiko tinggi. Standar tersebut setidaknya harus mencakup lima komponen utama.

Pertama, *AI risk assessment*, yaitu kewajiban melakukan identifikasi risiko kriminal sebelum sistem diimplementasikan. Kedua, *algorithmic audit*, yakni evaluasi berkala terhadap bias, opacity dan potensi manipulasi sistem. Ketiga, *explainability mechanism*, yaitu kewajiban menjaga keterjelasan logika keputusan AI agar output dapat ditelusuri. Keempat, *human oversight mechanism*, yakni keharusan menyediakan intervensi manusia pada keputusan berisiko tinggi. Kelima, *compliance documentation*, berupa pencatatan proses pengembangan dan deployment AI yang dapat digunakan dalam pembuktian hukum. Kewajiban-kewajiban tersebut memiliki implikasi penting. Dalam model regulasi yang direkonstruksi, absennya mekanisme compliance tidak hanya menimbulkan risiko administratif, tetapi dapat menjadi indikator awal keberadaan kesalahan pidana korporasi.

d. Rekonstruksi Model Liability: *Hybrid Criminal Liability Framework*

AI-assisted business crime tidak dapat direspons secara efektif melalui satu model liability tunggal. Kompleksitas teknologi menuntut pendekatan yang lebih elastis dan berbasis risiko. Oleh karena itu, penelitian ini mengusulkan *Hybrid Criminal Liability Framework* sebagai model pertanggungjawaban pidana yang menggabungkan beberapa basis liability secara simultan.

⁴⁹ Fabian Teichmann, dkk., *Compliance as a Form of Defense against Corporate Criminal Liability*, Journal of Economic Criminology, Vol.1 (2023).

Model hibrid ini terdiri dari tiga lapisan. Lapisan pertama adalah *fault-based liability*, yang tetap digunakan ketika terdapat intentional fraud, rekayasa sistem, atau instruksi eksplisit untuk melakukan kejahatan. Lapisan kedua adalah *negligence-based liability*, yang berlaku ketika korporasi gagal menjalankan kewajiban kehati-hatian dalam pengelolaan AI. Lapisan ketiga adalah *strict regulatory liability*, yang diterapkan pada sektor dengan risiko publik tinggi apabila kewajiban compliance tertentu diabaikan.⁵⁰

Keunggulan model hibrid terletak pada fleksibilitasnya. Hukum pidana tidak dipaksa memilih antara pendekatan klasik dan pendekatan modern, melainkan mampu menyesuaikan respons berdasarkan tingkat otonomi AI, tingkat risiko, serta sifat pelanggaran. Pendekatan ini juga lebih realistis untuk konteks Indonesia yang masih berada pada tahap transisi regulatif.

e. Harmonisasi Regulasi dan Penguatan Penegakan Hukum

Rekonstruksi regulasi tidak akan efektif tanpa harmonisasi antarrezim hukum. AI-assisted business crime bersifat lintas sektor dan tidak dapat ditangani secara eksklusif oleh hukum pidana. Karena itu, reformasi harus menciptakan integrasi antara regulasi pidana, perlindungan data, sektor keuangan, persaingan usaha dan tata kelola teknologi.

Selain harmonisasi normatif, kapasitas penegakan hukum juga perlu diperkuat. Aparat penegak hukum membutuhkan kompetensi baru dalam digital forensics, algorithmic auditing dan AI governance analysis. Tanpa penguatan kapasitas institusional, reformasi normatif berisiko berhenti sebagai perubahan tekstual yang tidak operasional.

Analisis yang bersifat rekonstruktif ini menunjukkan bahwasanya respons hukum pidana terhadap AI-assisted business crime tidak dapat diselesaikan dengan menggunakan pendekatan penal tradisional yang semata represif. Yang dibutuhkan ialah perubahan paradigma dari *reactive criminal enforcement* menuju *risk-responsive criminal governance*.

⁵⁰ N. Bhatt, *Crimes in the Age of Artificial Intelligence: a Hybrid Approach to Liability and Security in the Digital Era*, Journal of Digital Technologies and Law, Vol.3, No.1 (2025).

Dalam paradigma baru ini, hukum pidana tidak hanya berfungsi menghukum pelanggaran yang telah terjadi, tetapi juga membangun insentif institusional agar korporasi secara aktif mengelola risiko kriminal yang dihasilkan oleh sistem AI.

Dengan demikian, rekonstruksi regulasi hukum pidana Indonesia terhadap AI-assisted business crime harus dipahami sebagai reformasi struktural terhadap cara hukum mendefinisikan kesalahan, membangun pertanggungjawaban dan menilai kewajiban tata kelola korporasi. Reformasi tersebut pada akhirnya memperkuat tesis utama penelitian ini: pada era AI, pertanggungjawaban pidana korporasi tidak lagi cukup dipahami sebagai liability atas tindakan kriminal individual, melainkan sebagai liability atas kegagalan institusional dalam mengelola risiko algoritmik.

C. PENUTUP

Perkembangan Artificial Intelligence (AI) telah mentransformasi kejahatan bisnis menjadi kriminalitas berbasis algoritma yang semakin kompleks, adaptif dan sulit diatribusikan secara pidana. Indonesia hingga saat ini belum memiliki regulasi khusus mengenai AI, sementara pengaturan yang ada, seperti Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 11 Tahun 2008 juncto Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, belum secara eksplisit mengatur AI-assisted business crime. Oleh karena itu, pertanggungjawaban pidana korporasi perlu direkonstruksi melalui pendekatan *multi-layered accountability* dan *liability for algorithmic governance failure* agar lebih adaptif terhadap risiko kriminal berbasis AI.

DAFTAR PUSTAKA

Buku

- Abbott, Ryan dan Alexander Sarch. 2024. *Punishing Artificial Intelligence: Legal Fiction or Science Fiction, In Legal Aspects of Autonomous Systems: A Comparative Approach*. (Berlin: Springer International Publishing).
- Błachnio-Parzych, Anna dan Luigi Cornacchia. 2026. *Legal Protection against Financial Market Abuse: International and Local Perspectives*. (London: Routledge).
- Chakrawarti, Rajesh Kumar, dkk.. 2026. *Cognitive Cyber Crimes in the Era of Artificial Intelligence*. (Beverly: Scrivener Publishing LLC).
- Kaushik, Pooja, dkk.. 2025. *Financial Fraud and Manipulation: The Malicious Use of Deepfakes in Business, In Advances in Business Information Systems and Analytics*. (Hershey: IGI Global Scientific Publishing).
- McShane, Marilyn D. dan Frank P. Williams III. 2020. *The American Court System*. (London: Routledge).
- Sonali dan Gunjan. 2025. *Human Agency and Machine Logic: Reassessing Mens Rea in The Age of Algorithmic Decision-Making, In From Mens Rea to Machine Rea: Reimagining Criminal Culpability in Digital Age*. (Lunawada: Redshine Publication).

Publikasi

- Alluri, Ravi Kiran. *Detecting Synthetic Identity Fraud Via Multimodal Customer Data Integration*. Journal of Artificial Intelligence & Cloud Computing. Vol.1. No.1 (2022).
- Bailo, Paolo, dkk.. *A Review of Crime at Machine Speed: Criminological Aspects of Artificial Intelligence's Industrialisation of Deception*. Sci. Vol.8. No.3 (2026).
- Berghoff, Hartmut dan Uwe Spiekermann. *Shady Business: On the History of White-Collar Crime*. Business History. Vol.60. No.3 (2018).
- Bhatt, N. *Crimes in the Age of Artificial Intelligence: a Hybrid Approach to Liability and Security in the Digital Era*. Journal of Digital Technologies and Law. Vol.3. No.1 (2025).
- Caldwell, M., dkk.. *AI-Enabled Future Crime*. Crime Science. Vol.9. No.1 (2020).
- Damanik, Yanel Garsione. *Problematika Pencegahan dan Kejahatan di Bidang Ekonomi*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.1. No.4 (2020).
- Daraojimba, Rosita Eberechukwu, dkk.. *Forensic Accounting in the Digital Age: A U.S. Perspective: Scrutinizing Methods and Challenges in Digital Financial Fraud Prevention*. Finance & Accounting Research Journal. Vol.5. No.11 (2023).
- Cenyvesta, Marshella dan Ariawan Gunadi. *Konsep Tanggung Jawab Negara terhadap Kewajiban Melindungi Data Pribadi Masyarakat di Indonesia (Studi Kasus Kebocoran Data NPWP Masyarakat Indonesia)*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.5. No.12 (2024).

- Fisher, Sethard. *Economic Development and Crime: The Two May Be Associated as an Adaptation to Industrialism in Social Revolution*. The American Journal of Economics and Sociology. Vol.46. No.1 (1987).
- Fitriya, Riska, dkk.. *Melacak Jejak Pidana AI: Status Subjek Hukum dan Model Pertanggungjawaban di Indonesia*. As-Syar'i: Jurnal Bimbingan & Konseling Keluarga. Vol.8. No.1 (2026).
- Frans, Mardian Putra, dkk.. *Pertanggungjawaban Pidana Bank sebagai Pengguna Artificial Intelligence*. Jurnal USM Law Review. Vol.7. No.2 (2024).
- Ghazmi, Shabrina Fadiah. *Urgensi Pengaturan Artificial Intelligence pada Sektor Bisnis Daring di Indonesia*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.2. No.8 (2021).
- Gustryan, Muhammad dan Zainal Arifin Hoesein. *Peran Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi dalam Perlindungan Data dan Privasi di Era Ekonomi Digital*. Jurnal Minfo Polgan. Vol.14. No.2 (2025).
- Hamdi, Saiful, dkk.. *Implikasi Hukum Penggunaan Artificial Intelligence sebagai Bewijsmiddelen dalam Penegakan Hukum di Indonesia (Telaah Pragmatisme Abduksi)*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.4. No.10 (2023).
- Hasan, Zulfikar dan Diska Sendi Marisna. *Artificial Intelligence: Making Crime Easier in The World of Finance?.* AL-ARBAH: Journal of Islamic Finance and Banking. Vol.6. No.2 (2024).
- Hermanto, Halim dan Lolita Fitriyana. *Pengaturan Penyitaan Aset Kripto sebagai Hasil Tindak Pidana Pencucian Uang di Indonesia*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.6. No.7 (2025).
- Ibrahim, Muhammad Kautsar, dkk.. *Urgensi Pembaruan Hukum dalam Menghadapi Kejahatan yang Melibatkan Teknologi Kecerdasan Buatan AI*. Journal of Legal, Political and Humanistic Inquiry. Vol.1. No.2 (2025).
- Irawati, Nurulhuda, Ismansyah dan Nani Mulyati. *Pertanggungjawaban Pidana Deepfake Porn Berbasis AI: Studi Perbandingan dan Implikasi Global*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.7. No.1 (2026).
- Juniarso, Dian, dkk.. *Reformasi Kebijakan Pidana Nasional terhadap Kejahatan Siber Berbasis AI melalui Pendekatan Hukum Progresif*. Jurnal Impresi Indonesia. Vol.5. No.1 (2026).
- Khaund, Bhaskardeep. *AI and Identity Security: The Threat of Deepfakes and the Future of Authentication*. World Journal of Advanced Engineering Technology and Sciences. Vol.15. No.3 (2025).
- Khuan, Hendri. *Void in Law: Criminal Regulation Vacuum on the Detrimental Impact of AI Artificial Intelligence*. Journal of Strafvordering Indonesian. Vol.2. No.3 (2025).
- King, Thomas C., dkk.. *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*. Science and Engineering Ethics. Vol.26. No.1 (2020).
- Llorca, David Fernández, dkk.. *Liability Regimes in the Age of AI: a Use-Case Driven Analysis of the Burden of Proof*. Journal of Artificial Intelligence Research. Vol.76 (2023).

- Lokanan, Mark. *Ai-Driven Detection of Industry-Specific Financial Fraud: A Theory-Informed NLP Approach*. *Journal of White Collar and Corporate Crime*. Vol.0. No.0 (2026).
- Lowe, Richard John. *Anti-Money Laundering – The Need for Intelligence*. *Journal of Financial Crime*. Vol.24. No.3 (2017).
- Mahmud, Arif. *Application and Criminalization of the Artificial Intelligence in Business: Recommendation to Counter the Regulatory Challenges*. *Journal of Applied Security Research*. Vol.18. No.4 (2023).
- Mangrio, Imran Ali dan Liaquat Ali Abro. *Multi Faceted White Collar Crime Eating Country's Economic Fabric Like Termite*. *Al Meezan Research Journal of Social Sciences*. Vol.2. No.2 (2022).
- Meliana, Yang. *Dialektika Sistem Peradilan terhadap Analisis Kritis Perbandingan Litigasi Virtual dan Konvensional dalam Perspektif Hak Pembelaan Terdakwa*. *Rewang Rencang: Jurnal Hukum Lex Generalis*. Vol.6. No.7 (2025).
- _____. *Urgensi Formulasi Perlindungan Hukum dan Kepastian Pidana terhadap Pengaturan Tindak Pidana Deepfake dalam Sistem Hukum Pidana Nasional*. *Rewang Rencang: Jurnal Hukum Lex Generalis*. Vol.6. No.7 (2025).
- Nasman, dkk.. *Etika dan Pertanggungjawaban Penggunaan Artificial Intelligence di Indonesia*. *Rewang Rencang: Jurnal Hukum Lex Generalis*. Vol.5. No.10 (2024).
- Nurjaman, Iman dan Yuyut Prayuti. *Celah Regulasi Penegakan Hukum dalam Mengatasi Pencucian Uang dari Kejahatan Ekonomi melalui Aset Digital di Indonesia*. *Rewang Rencang: Jurnal Hukum Lex Generalis*. Vol.6. No.7 (2025).
- Nusanto, Tri Suyud dan Aloysius Wisnubroto. *Criminal Law Challenges and Solutions in Artificial Intelligence-Based Crime Prevention in Indonesia*. *Multidisciplinary Indonesian Center Journal*. Vol.3. No.1 (2026).
- Pakpahan, Dosni Ana Ragita dan Anis Widyawati. *Reformulation of Cybercrime Regulations in The Misuse of Artificial Intelligence in Indonesia*. *Law Research Review Quarterly*. Vol.12. No.1 (2026).
- Peters, Uwe. *Explainable AI Lacks Regulative Reasons: Why AI and Human Decision-Making Are Not Equally Opaque*. *AI and Ethics*. Vol.3. No.3 (2023).
- Purnomo, Hadi. *Criminal Liability for the Use of Artificial Intelligence in Indonesia*. *Jurnal Info Sains: Informatika dan Sains*. Vol.13. No.3 (2023).
- Rasji dan Rupertus Arvinci Ngabut. *Filsafat Positivisme Hukum dalam Pemberantasan Pencucian Uang: Analisis Kepastian Hukum dan Implementasi di Indonesia*. *Rewang Rencang: Jurnal Hukum Lex Generalis*. Vol.5. No.10 (2024).
- Saifullah, dkk.. *The Evaluation of The Indonesian Fintech Law from The Perspective of Regulatory Technology Paradigms to Mitigate Illegal Fintech*. *Jurisdictie: Jurnal Hukum dan Syariah*. Vol.14. No.2 (2024).
- Sattar, Sadia. *The Next Frontier of Cybercrime Law for Artificial Intelligence and Criminal Liability*. *International Journal of Law and Policy*. Vol.3. No.8 (2025).

Suseno, Sigid, dkk.. *Cybercrime in the New Criminal Code in Indonesia*. Cogent Social Sciences. Vol.11. No.1 (2025).

Teichmann, Fabian, dkk.. *Compliance as a Form of Defense against Corporate Criminal Liability*. Journal of Economic Criminology. Vol.1 (2023).

Weimer daniel, dkk.. *Scaling of End-To-End Governance Risk Assessments for AI Systems (Practitioner Track)*. Prosiding Symposium on Scaling AI Assessments (2024).

Yatini, dkk.. *Reformulasi Konstruksi Pidana dalam Menjerat Pelaku Tindak Pidana Korporasi*. Jurnal Hukum dan Pembangunan Ekonomi. Vol.7. No.1 (2019).

Karya Ilmiah

Zweers, Benjamin, dkk.. 2025. *The AI-Fraud Diamond: A Novel Lens for Auditing Algorithmic Deception*. Artikel Ilmiah. Ithaca: arXiv.

Website

Maklu-Online. *Corporate Criminal Liability for AI Related Crimes: Possible Legal Techniques and Obstacles*. diakses dari <https://www.maklu-online.eu/en/tijdschrift/ridp/2023/traditional-criminal-law-categories-and-ai-crisis-/corporate-criminal-liability-ai-related-crimes-pos/?>. diakses pada 5 Juli 2026.

Sumber Hukum

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251. Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1. Tambahan Lembaran Negara Republik Indonesia Nomor 6842.

Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial.