Muhammadiyah Law Review
P-ISSN: 2549-113X, E-ISSN: 2580-166X
Vol. 10 No. 2 (2026)

Pertanggungjawaban Pidana Atas Pelanggaran Data Pribadi Berbasis Kecerdasan Buatan Dalam Perspektif Perbandingan Hukum Pidana (Indonesia, Uni Eropa dan Singapura)

Abdul Aziz Pamaungkas[1], Yulianto Pamungkas[2], Javan Agustian Setyagraha[3], Sumarno[4], Moch. Eko Setiyo B.U[5]
Universitas Boyolali[1,2,3,4,5]
Corresponding Author: abdulazizpamungkas029@gmail.com

Abstract

The rapid advancement of artificial intelligence (AI) technology presents a fundamental paradox: on one hand, it drives efficiency and innovation; on the other, it creates unprecedented potential for large-scale exploitation of personal data. Indonesia's positive criminal law comprising the New Penal Code (Law No. 1 of 2023), the Electronic Information and Transactions Law (EIT Law), and the Personal Data Protection Law (PDP Law No. 27 of 2022)—faces serious challenges in constructing criminal liability for data violations mediated by autonomous AI systems. This research aims to analyse: (1) the construction of criminal liability for AI-based personal data violations under Indonesia's positive criminal law; and (2) a comparative assessment of criminal law enforcement effectiveness in the AI and personal data domain between Indonesia and the European Union (GDPR and EU AI Act) and Singapore (PDPA). A normative-doctrinal legal research method was employed, using statute, conceptual, and comparative approaches. Findings reveal that Indonesia suffers from three critical regulatory gaps: (a) the absence of a legally cognizable definition of an 'AI system' for criminal liability purposes; (b) ambiguity in establishing mens rea for autonomous data processing; and (c) an unclear strict liability mechanism for corporations in mass data violations. Compared to the EU and Singapore legal regimes, Indonesia's criminal law construction remains reactive and has yet to adopt by-design accountability principles. The research recommends: the issuance of a Government Regulation under the PDP Law explicitly addressing AI-based offences; the establishment of an independent AI Supervisory Authority; and the codification of a vicarious criminal liability doctrine for corporations in digital technology regulations.

Keywords: *Artificial Intelligence, Criminal Liability, Personal Data Protection*

Abstrak

Perkembangan teknologi kecerdasan buatan (artificial intelligence/AI) membawa paradoks fundamental di satu sisi mendorong efisiensi dan inovasi, di sisi lain membuka potensi eksploitasi data pribadi dalam skala yang belum pernah terjadi sebelumnya. Hukum pidana positif Indonesia, yang terdiri atas KUHP Baru (UU No. 1 Tahun 2023), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang Perlindungan Data Pribadi (UU PDP No. 27 Tahun 2022), menghadapi tantangan serius dalam mengkonstruksi pertanggungjawaban pidana terhadap

Creative Commons Attribution 4.0 International License

pelanggaran data yang dimediasi oleh sistem AI yang bersifat otonom. Penelitian ini bertujuan menganalisis: (1) konstruksi pertanggungjawaban pidana terhadap pelanggaran data pribadi berbasis AI dalam hukum pidana positif Indonesia; dan (2) perbandingan efektivitas penegakan hukum pidana di bidang AI dan data pribadi antara Indonesia dengan Uni Eropa (GDPR dan EU AI Act) serta Singapura (PDPA). Metode yang digunakan adalah penelitian hukum normatif-doktrinal dengan pendekatan perundang-undangan, konseptual, dan komparatif. Hasil penelitian menunjukkan bahwa Indonesia mengalami tiga kekosongan regulasi kritis: (a) ketiadaan definisi 'sistem AI' yang dapat dimintai pertanggungjawaban pidana; (b) ambiguitas mens rea dalam pemrosesan data otonom; dan (c) ketidakjelasan mekanisme strict liability korporasi dalam pelanggaran data masif. Dibandingkan dengan rezim hukum UE dan Singapura, konstruksi pidana Indonesia bersifat reaktif dan belum mengadopsi prinsip by-design accountability. Penelitian ini merekomendasikan pembentukan Peraturan Pemerintah turunan UU PDP yang secara eksplisit mengatur tindak pidana berbasis AI, pembentukan Otoritas Pengawas AI independen, serta kodifikasi doktrin vicarious criminal liability korporasi dalam regulasi teknologi digital.

Kata kunci: Kecerdasan Buatan, Pertanggungjawaban Pidana, Perlindungan Data Pribadi.

A. Pendahuluan

Revolusi industri keempat yang didorong oleh kecerdasan buatan telah menempatkan data pribadi sebagai komoditas paling berharga dalam ekosistem ekonomi digital global. Sistem algoritma AI mampu memproses, menganalisis, dan mengeksploitasi miliaran titik data personal dalam hitungan detik, menciptakan profil psikografis individu yang bahkan lebih komprehensif dari apa yang subjek data itu sendiri ketahui tentang dirinya. Fenomena ini menimbulkan permasalahan hukum mendasar yang belum terjawab tuntas oleh rezim hukum pidana konvensional terkait yang bertanggung jawab secara pidana ketika sebuah sistem AI mengeksploitasi data pribadi tanpa persetujuan pemiliknya.[1]

Kasus-kasus nyata mengilustrasikan urgensi persoalan ini dengan gamblang. Penggunaan deepfake berbasis AI generatif (generative AI) untuk menciptakan konten pornografi non-konsensual, praktik micro-targeting berbasis profil psikografis data curian dalam konteks politik (seperti skandal *Cambridge Analytica)*, hingga eksploitasi data biometrik oleh sistem pengenalan wajah tanpa izin, semuanya merepresentasikan kategori baru kejahatan yang disebut sebagai '*dignity crimes'* dalam literatur hukum kontemporer.[2] Karakteristik kejahatan-kejahatan ini adalah keterlibatan entitas non-manusia (algoritma AI) dalam eksekusi aktus reus, sehingga konstruksi pertanggungjawaban pidana konvensional yang bertumpu pada asas cogitationis poenam nemo patitur dan actus non facit reum nisi mens sit rea mengalami kebuntuan epistemologis yang serius.

Di Indonesia, regulasi perlindungan data pribadi relatif baru lahir. Undang-

[1] Sayyed, H. Artificial intelligence and criminal liability in India: exploring legal implications and challenges. Cogent Social Sciences, (2024), hlm. 10.

[2] Danielle Keats Citron, The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age (W.W. Norton & Company, 2022), hlm. 45-67. Citron mengklasifikasikan penyalahgunaan AI terhadap data pribadi sebagai 'kejahatan bermartabat' (dignity crimes) yang bersifat sistemik.

Creative Commons Attribution 4.0 International License

Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) baru mulai berlaku efektif pada Oktober 2024, setelah melewati masa transisi dua tahun.[3] Meski demikian, pembuat undang-undang telah mengantisipasi tantangan teknologi dengan memasukkan ketentuan tentang pemrosesan data berbasis otomasi, namun ketentuan-ketentuan ini belum memadai untuk menjawab tantangan spesifik yang ditimbulkan oleh AI dalam konteks hukum pidana.

Hukum pidana konvensional Indonesia didesain untuk subjek hukum yang bersifat personal dan memiliki kehendak bebas (*free will*), baik berupa orang perorangan (*naturlijk persoon*) maupun korporasi sebagai badan hukum (*rechtspersoon*).[4] Ketika sebuah sistem AI bertindak secara otonom membuat keputusan, melakukan pemrosesan data, atau bahkan menghasilkan konten palsu berbasis deepfake tanpa instruksi eksplisit dari manusia timbul kekosongan hukum (legal vacuum) yang fundamental AI bukan subjek hukum, namun perilakunya dapat menimbulkan akibat hukum yang merugikan orang lain.

Kekosongan hukum ini mencakup tiga dimensi pertama, ketiadaan definisi sistem AI dalam konstruksi norma pidana yang ada, sehingga penegak hukum mengalami kesulitan dalam mengidentifikasi perbuatan pidana yang dapat dinisbatkan kepada pengembang atau pengguna AI. Kedua, ambiguitas mens rea ketika keputusan diambil oleh algoritma apakah niat jahat pengembang AI harus dibuktikan pada saat pemrograman, atau pada saat penggunaan, atau cukup dibuktikan melalui hasil strict liability.[5] Ketiga, ketiadaan mekanisme pertanggungjawaban korporasi yang memadai ketika perusahaan teknologi mengeksploitasi data pribadi melalui sistem AI yang beroperasi di balik 'kotak hitam' (*black box*) algoritma yang tidak transparan. Dalam KUHP Baru (UU No. 1 Tahun 2023) yang mulai berlaku pada Januari 2026 memang mengandung kemajuan signifikan dalam hal pertanggungjawaban korporasi, namun belum secara eksplisit mengatur pertanggungjawaban pidana berbasis AI.[6] UU ITE pun menghadapi keterbatasan serupa: pasal-pasalnya lebih berfokus pada akses ilegal dan manipulasi konten digital secara manual, bukan pada pemrosesan data masif berbasis algoritma otonom.

Indonesia tidak sendirian menghadapi tantangan ini, namun yurisdiksi lain telah selangkah lebih maju. Uni Eropa telah mengadopsi EU AI Act (*Regulation* (EU) 2024/1689) sebagai regulasi AI komprehensif pertama di dunia yang menggunakan pendekatan berbasis risiko, dan mengintegrasikannya dengan GDPR sebagai kerangka perlindungan data yang telah terbukti efektif.[7] Singapura, sebagai pusat teknologi Asia Tenggara, telah memperbarui *Personal Data Protection Act* (PDPA) pada 2020 dan mengembangkan kerangka tata kelola AI yang pragmatis melalui pendekatan *soft law* yang khas *common law*.[8]

---

[3] Pasal 1 angka 1 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mendefinisikan data pribadi sebagai 'data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya.

[4] Eurike Hailtik, A.G., & Afifah, W. Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia. Asian Journal of Social and Humanities, (2024).

[5] Dvornikova, P., & Osadchaya, A. Artificial Intelligence And The Law: The Challenges Of Establishing Criminal Liability In The Digital Age. Juridical scientific and electronic journal. (2024).

[6] Ginting, Y. Akuntabilitas Pidana di Era Penyalahgunaan Kecerdasan Buatan ditinjau dari Asas Legalitas. The Prosecutor Law Review, 3(3)., 2025.

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation/GDPR), OJ L 119, 4.5.2016, p. 1-88

[8] Personal Data Protection Act 2012 (PDPA Singapore), No. 26 of 2012, sebagaimana diubah

Creative Commons Attribution 4.0 International License

Berdasarkan uraian latar belakang di atas, penelitian ini merumuskan dua permasalahan hukum sebagai berikut (1) Bagaimana pertanggungjawaban pidana terhadap pelanggaran data pribadi yang melibatkan teknologi kecerdasan buatan dalam hukum pidana positif Indonesia (UU PDP, KUHP Baru, dan UU ITE), (2) Apa kelebihan dan kelemahan penegakan hukum pidana terkait AI dan data pribadi di Indonesia jika dibandingkan dengan regulasi di Uni Eropa dan Singapura, dan bagaimana rekonstruksi hukum pidana Indonesia ke depan guna menutup kesenjangan regulasi yang ada. Studi komparatif terhadap kedua yurisdiksi ini relevan karena tiga alasan: (1) Uni Eropa mewakili pendekatan civil law yang berkarakter preventif dan berbasis hak asasi (*rights-based approach*) yang konvergen dengan tradisi hukum Indonesia; (2) Singapura sebagai negara ASEAN yang berbagi konteks geopolitik dan model bisnis digital yang serupa dengan Indonesia namun dengan kapasitas penegakan hukum yang lebih kuat; dan (3) baik GDPR maupun EU AI Act telah mulai diakui sebagai 'standar emas' (*gold standard*) global yang mempengaruhi perkembangan regulasi AI di seluruh dunia, termasuk di kawasan Asia Tenggara.

B. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif-doktrinal (*doctrinal legal research*) yang berfokus pada analisis kritis terhadap bahan hukum primer berupa peraturan perundang-undangan dan putusan pengadilan, serta bahan hukum sekunder berupa doktrin, literatur ilmiah, dan laporan lembaga internasional.[9] Tiga pendekatan diterapkan secara sinergis: pertama, pendekatan perundang-undangan (*statute approach*) yang menganalisis ketentuan-ketentuan dalam UU PDP No. 27/2022, KUHP Baru No. 1/2023, UU ITE No. 19/2016, serta peraturan pelaksanaannya; kedua, pendekatan konseptual (*conceptual approach*) yang merujuk pada doktrin hukum pidana tentang *mens rea, actus reus, strict liability*, dan *vicarious liability* dalam konteks entitas AI; ketiga, pendekatan komparatif (comparative approach) yang membandingkan sistem hukum Indonesia secara fungsional (*functional comparison*) dengan kerangka hukum Uni Eropa (GDPR dan EU AI Act) dan Singapura (PDPA dan National AI Strategy) untuk mengidentifikasi persamaan, perbedaan, dan kemungkinan adopsi *best practices*. Analisis dilakukan secara kritis dan evaluatif, dengan mengukur efektivitas masing-masing sistem hukum berdasarkan tiga variabel: (a) kejelasan rumusan delik; (b) kemampuan penangkapan subjek hukum yang tepat; dan (c) proporsionalitas sanksi terhadap tingkat risiko teknologi

C. Anatomi Kejahatan Data Pribadi Berbasis AI dan Konstruksi Pidana di Indonesia

Pemahaman terhadap anatomi kejahatan data berbasis AI mensyaratkan pemetaan tipologi yang cermat. Setidaknya terdapat empat kategori utama kejahatan yang relevan dalam konteks Indonesia saat ini. Pertama, kejahatan pemrosesan data masif tanpa persetujuan (*unauthorized bulk data processing*) penggunaan algoritma machine learning untuk *scraping* dan agregasi data pribadi dari berbagai sumber tanpa dasar hukum yang sah, sering dilakukan oleh perusahaan fintech ilegal atau platform

terakhir oleh Personal Data Protection (Amendment) Act 2020. PDPA Singapura mengadopsi pendekatan berbasis akuntabilitas dengan kewajiban notifikasi pelanggaran data yang ketat.

[9] Soerjono Soekanto dan Sri Mamudji, Penelitian Hukum Normatif: Suatu Tinjauan Singkat (Jakarta: Rajawali Pers, 2011), hal. 13-14; Bandingkan dengan Terry Hutchinson, "Doctrinal Legal Research: Focus on Method," dalam Research Methods for Law, ed. Mike McConville dan Wing Hong Chui (Edinburgh: Edinburgh University Press, 2017), hal. 9.

Creative Commons Attribution 4.0 International License

social scoring. Kedua, *deepfake crime* penggunaan AI generatif (*Generative Adversarial Networks*/GANs) untuk menciptakan konten sintetis palsu yang menggunakan identitas, wajah, atau suara seseorang tanpa persetujuan. Kejahatan ini memiliki dimensi berganda pelanggaran data biometrik (yang termasuk data sensitif menurut Pasal 4 UU PDP) sekaligus potensi pencemaran nama baik atau pornografi non-konsensual.[10] Ketiga, profiling ilegal berbasis AI: penggunaan algoritma untuk membangun profil psikografis, politik, atau finansial individu dari data yang dikumpulkan secara ilegal, kemudian digunakan untuk micro-targeting dalam konteks periklanan, politik, atau penipuan (*fraud*). Keempat, automated decision-making crime: penggunaan sistem AI untuk membuat keputusan otomatis yang berdampak signifikan pada seseorang misalnya penolakan kredit, pemecatan pekerjaan, atau penolakan akses layanan publik berdasarkan pemrosesan data pribadi yang tidak sah atau diskriminatif.[11]

UU PDP menandai babak baru perlindungan data di Indonesia dengan memuat ketentuan pidana yang berdiri sendiri (*lex specialis*). Pasal 67 ayat (1) mengancam pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp5.000.000.000,00 bagi pelaku yang 'dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya.[12] Pasal 68 menambahkan sanksi pidana atas penggunaan data pribadi yang mengakibatkan kerugian subjek data, sementara Pasal 69 mengatur pidana atas pemalsuan data pribadi. Secara komparatif dengan KUHP Baru dan UU ITE, ketentuan pidana UU PDP memiliki keunggulan dalam hal spesifisitas subjek hukum dan gradasi sanksi.[13] Namun, terdapat kelemahan struktural yang kritis pertama, UU PDP tidak mendefinisikan 'sistem kecerdasan buatan' sebagai instrumen kejahatan, sehingga ketika pelanggaran dilakukan melalui sistem AI otonom, jaksa harus membuktikan nexus kausal antara keputusan pemrograman manusia dan output AI yang merugikan sebuah tantangan teknis-yuridis yang tidak ringan; kedua, ketentuan tentang pertanggungjawaban korporasi dalam Pasal 70 UU PDP bersifat *vicarious* dan tidak mengatur *strict liability*, sehingga korporasi yang menggunakan AI dapat berargumen bahwa pelanggaran terjadi di luar kehendak dan kontrol manajemennya; ketiga, tidak ada ketentuan yang mengatur DPIA (*Data Protection Impact Assessment*) sebagai kewajiban *ex ante* yang kegagalannya dapat dikriminalisasi, berbeda dengan pendekatan GDPR.[14]

Persoalan paling fundamental dalam hukum pidana AI adalah rekonstruksi elemen *mens rea* dan *actus reus* ketika agen pelaksana kejahatan adalah algoritma,

[10] Pamungkas, A. A., Sutarni, N., & Pranawa, B. Legal analysis of deepfake technology in Indonesia from the perspective of fair and civilized humanity. Pena Justisia: Media Komunikasi Dan Kajian Hukum, 24(1), 2025, hlm. 4562-4574.

[11] Auliya, S.F., Kudina, O., Ding, A.Y., & van de Poel, I. AI versus AI for democracy: exploring the potential of adversarial machine learning to enhance privacy and deliberative decision-making in elections. AI and Ethics, 5, (2024), hlm. 2801 - 2813.

[12] Pasal 67 ayat (1) jo. Pasal 65 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mengancam pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah) bagi pelaku yang memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan tujuan menguntungkan diri sendiri.

[13] Pasal 407 dan Pasal 408 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Baru) mengatur tentang pengrusakan dan penghancuran data elektronik sebagai tindak pidana dengan ancaman penjara hingga 4 tahun.

[14] Pasal 17 ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mengatur bahwa pemrosesan data pribadi oleh sistem otomasi harus disertai penilaian dampak perlindungan data (Data Protection Impact Assessment/DPIA).

Creative Commons Attribution 4.0 International License

bukan manusia. Doktrin hukum pidana klasik mensyaratkan kesatuan antara keduanya dalam diri satu subjek hukum yang sama (*coincidence rule*).[15] Dalam konteks AI, 'perbuatan' (*actus reus*) dilakukan oleh sistem algoritma, sementara 'kehendak' atau 'niat' (*mens rea*) harus ditelusuri mundur ke aktor manusia yang memprogram, mengerahkan, atau mengoperasikan sistem tersebut. Tiga model *attribution of criminal liability* dapat dikonstruksikan dalam konteks AI (a) Model *Developer Liability*, developer AI dimintai pertanggungjawaban atas desain sistem yang memungkinkan pelanggaran data *mens rea* dibuktikan pada fase pemrograman (design intent); (b) Model *Operator Liability*: operator atau pengguna AI yang mengerahkan sistem untuk tujuan yang mengakibatkan pelanggaran data *mens rea* dibuktikan pada *fase deployment* (*operational intent*); (c) *Model Strict Liability* Korporasi yang memperoleh manfaat ekonomi dari pemrosesan data oleh AI bertanggung jawab secara pidana tanpa perlu membuktikan *mens rea*, dengan dasar pertanggungjawaban adalah risiko bisnis yang diciptakannya.[16] Hukum pidana Indonesia saat ini tidak memiliki dasar normatif yang eksplisit untuk menerapkan model ketiga (*strict liability*), meskipun Pasal 97 KUHP Baru mengatur pertanggungjawaban korporasi secara umum. Ketiadaan ketentuan *strict liability* dalam konteks data AI menciptakan insentif negatif bagi korporasi untuk 'menyembunyikan' pertanggungjawaban di balik kompleksitas algoritma fenomena yang oleh Balkin disebut sebagai '*algorithmic shield*'.[17]

UU ITE memberikan beberapa jangkar normatif relevan: Pasal 35 mengatur manipulasi informasi/dokumen elektronik (*framing* yang dapat diperluas untuk *deepfake*), Pasal 32 mengatur transmisi data elektronik tanpa izin, dan Pasal 46 mengatur akses ilegal ke sistem elektronik.[18] Namun, seluruh pasal ini didesain untuk perbuatan aktif manusia, bukan untuk sistem otonom. Yurisprudensi yang ada pun belum pernah menerapkan UU ITE dalam konteks pelanggaran data berbasis AI generatif. KUHP Baru yang mulai berlaku 2 Januari 2026 membawa pembaruan penting. Pasal 407-408 mengatur perusakan sistem elektronik, sementara Bab tentang pertanggungjawaban korporasi (Pasal 97-106) memperluas definisi 'tindak pidana korporasi' secara signifikan. Akan tetapi, KUHP Baru tetap tidak mendefinisikan AI sebagai subjek hukum ataupun instrumen khusus dalam konstruksi delik. Dengan demikian, penegak hukum harus beroperasi dalam ketidakpastian konseptual yang berpotensi menimbulkan pelanggaran asas legalitas *lex certa* dan *lex stricta*.

D. Studi Komparatif Indonesia dengan Uni Eropa dan Singapura

Uni Eropa membangun rezim perlindungan data berbasis AI di atas dua pilar regulasi yang saling melengkapi: GDPR (berlaku sejak Mei 2018) yang mengatur perlindungan data secara umum, dan EU AI Act (berlaku sejak Agustus 2024) yang mengatur tata kelola sistem AI secara sektoral berdasarkan tingkat risiko. GDPR memperkenalkan sejumlah prinsip revolusioner yang relevan untuk konteks AI: *data*

[15] Divino, S.B. Critical considerations on Artificial Intelligence liability: e-personality propositions., 2020

[16] Eurike Hailtik, A.G., & Afifah, W. (2024), Op.Cit.

[17] Jack Balkin, 'The Three Laws of Robotics in the Age of Big Data', Ohio State Law Journal, Vol. 78, No. 5 (2017), hlm. 1217-1241. Balkin mengajukan kerangka 'three laws' untuk AI: transparansi, non-diskriminasi, dan akuntabilitas sebagai prinsip dasar regulasi.

[18] Pasal 35 dan Pasal 46 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 35 mengancam pidana atas manipulasi informasi elektronik; Pasal 46 mengancam pidana atas akses ilegal ke sistem elektronik.

Creative Commons Attribution 4.0 International License

protection by design and by default (Pasal 25), yang mewajibkan pengembang AI untuk mengintegrasikan perlindungan data sejak fase perancangan sistem; *Data Protection Impact Assessment*/DPIA (Pasal 35), yang wajib dilakukan sebelum penerapan sistem pemrosesan data otomatis berskala besar; dan hak atas penjelasan atas keputusan otomatis (Pasal 22), yang memberikan hak kepada subjek data untuk tidak tunduk pada keputusan yang sepenuhnya otomatis tanpa intervensi manusia.[19]

EU AI Act mengklasifikasikan sistem AI dalam empat tingkat risiko: (1) *Unacceptable Risk* (dilarang sepenuhnya, mencakup AI untuk social scoring dan manipulasi bawah sadar); (2) *High Risk* (wajib mematuhi persyaratan ketat, mencakup biometrik, seleksi kerja, dan kredit); (3) *Limited Risk* (kewajiban transparansi, mencakup *chatbot* dan *deepfake*); (4) *Minimal Risk* (tidak diatur secara khusus) Pelanggaran ketentuan AI Act dapat dikenai denda administratif hingga €35 juta atau 7% dari total omset global tahunan korporasi jauh melampaui ancaman pidana dalam UU PDP Indonesia.[20] Dalam dimensi hukum pidana, GDPR tidak secara langsung mengatur sanksi pidana, namun Pasal 84 mengharuskan setiap negara anggota untuk menetapkan sanksi pidana atas pelanggaran GDPR yang tidak tercakup dalam sanksi administratif. Jerman, misalnya, menetapkan pidana penjara hingga 3 tahun untuk pelanggaran serius; Prancis dan Italia mengatur pidana atas pemrosesan data sensitif tanpa izin. Integrasi ini menciptakan ekosistem hukum yang bersifat *multi-track*: jalur administratif (denda) dan jalur pidana berjalan paralel, sehingga tidak ada 'celah impunitas' bagi pelanggar.

Singapura mengadopsi pendekatan yang berbeda secara fundamental regulasi berbasis *accountability* dan bukan berbasis *rights*, dengan penekanan pada tanggung jawab organisasional daripada hak individual. Mewajibkan setiap organisasi untuk menunjuk *Data Protection Officer* (DPO), menerapkan kebijakan perlindungan data yang komprehensif, dan melaporkan pelanggaran data dalam 3 hari setelah penemuan.[21] Dalam konteks AI, Singapura tidak memiliki regulasi AI yang mengikat secara hukum (*legally binding AI regulation*) seperti EU AI Act. Sebagai gantinya, Singapura mengembangkan *Model AI Governance Framework* (MAIGF) yang bersifat sukarela (*voluntary*) dan berbasis prinsip, yang memungkinkan industri mengadopsi standar tata kelola AI secara fleksibel.[22] Pendekatan ini mencerminkan filosofi *Common Law* yang menekankan *ex post accountability* (pertanggungjawaban setelah kejadian) dibanding *ex ante regulation* (pencegahan melalui regulasi ketat sebelum teknologi digunakan).

Dari perspektif penegakan pidana, PDPA Singapura memberikan denda administratif hingga $1 juta (dan kenaikan hingga 10% omset tahunan pasca-amandemen 2020), serta mengatur *enhanced criminal penalties* bagi individu yang secara sengaja menyebabkan organisasi melanggar PDPA mengisi celah 'individual *accountability*' yang lemah dalam regulasi korporasi. Inovasi kritis PDPA 2020

[19] European Data Protection Board (EDPB), Guidelines 02/2022 on the Application of Article 65(1)(a) GDPR (Brussels: EDPB, 2022). Panduan ini mengatur mekanisme konsistensi dan kerja sama antar-otoritas pengawas data di Eropa dalam menangani pelanggaran lintas batas.

[20] Anggie Irfansyah, Ketika AI Berhadapan dengan Hukum:Apa yang Harus Diketahui Bisnis Indonesia Sebelum Terlambat, Inixindo Jogja, 2026, Diakses melalui https://inixindojogja.co.id/ketika-ai-berhadapan-dengan-hukum-apa-yang-harus-diketahui-bisnis-indonesia-sebelum-terlambat/, pada 17 juni 2026, pukul 19.56 WIB.

[21] Rahmah, A. P. A., Anggraini, P. O., & Hasbi, M. "Perlindungan Data Pribadi Sebagai Hak Asasi Manusia di Era Digital: Analisis dan Perbandingan Indonesia dan Singapura". Al-Zayn: Jurnal Ilmu Sosial & Hukum, 4(3), (2026), hlm. 3242-3249.

[22] Lim, S.S., & Chng, G. Verifying AI: will Singapore's experiment with AI governance set the benchmark? Communication Research and Practice, 10, (2024), hlm. 297 - 306.

Creative Commons Attribution 4.0 International License

adalah pengenalan *deemed consent by notification* yang relevan untuk AI: penggunaan data untuk analitik berbasis AI dapat dilanjutkan sepanjang subjek data diberitahu dan tidak keberatan dalam jangka waktu tertentu.[23]

Perbandingan ketiga sistem hukum dapat divisualisasikan melalui empat variabel penegakan hukum pidana AI :

Tabel 1. Matriks Perbandingan Sistem Hukum Pidana AI Indonesia, UE dan Singapura

Variabel	Indonesia (UU PDP & KUHP Baru)	Uni Eropa (GDPR & EU AI Act)	Singapura (PDPA)
Definisi Sistem AI dalam Norma Pidana	Tidak ada (legal vacuum)	Ada (Pasal 3 EU AI Act)	Tidak ada (*soft law*)
Strict Liability Korporasi	Tidak eksplisit	GDPR Pasal 82: *Presumption of Liability*	PDPA: *Organizational Accountability*
Sanksi Maksimum	Penjara 6 Tahun + Denda Rp. 6 M (UU PDP)	Denda €35 juta / 7% *global turnover*	Denda S$1 juta / 10% omset
DPIA Wajib	Ada (Pasal 17 UU PDP), tanpa sanksi pidana	Ada (Pasal 35 GDPR), pelanggaran dapat dipidana	Tidak ada kewajiban formal
Deepfake Regulation	Tersirat dalam Pasal 35 UU ITE	Eksplisit dalam EU AI Act (*High-Risk*)	Belum ada regulasi spesifik
Otoritas Independen	Belum dibentuk (transisi 2024)	EDPB + Otoritas Nasional	PDPC (aktif dan berpengalaman)

Sistem hukum Uni Eropa unggul dalam hal *comprehensiveness* dan *preventive orientation*: integrasi GDPR-AI Act menciptakan kerangka hukum yang menutup hampir semua celah regulasi yang mungkin dieksploitasi oleh aktor jahat. Prinsip *by-design accountability* memastikan bahwa perlindungan data menjadi bagian intrinsik dari arsitektur teknis AI, bukan sekadar kewajiban kontraktual pasca-penggunaan.[24] Kelemahannya adalah biaya kepatuhan (*compliance cost*) yang tinggi yang dapat menghambat inovasi AI oleh startup dan UKM.

Singapura unggul dalam *regulatory agility* dan *industry-friendly approach* model tata kelola AI berbasis *soft law* yang fleksibel memungkinkan industri bergerak cepat beradaptasi dengan perkembangan teknologi tanpa terbebani kewajiban prosedural yang rigit. Kelemahannya adalah lemahnya *rights-based protection*: dalam sistem ini, kepentingan industri sering kali mendominasi kepentingan subjek data, dan mekanisme individual redress masih terbatas.[25] Indonesia, secara jujur, berada pada tahap paling awal dari ketiga yurisdiksi ini. UU PDP memang telah memberikan fondasi regulasi, namun ketidakhadiran otoritas pengawas yang fungsional, ketidakjelasan norma pidana berbasis AI, dan keterbatasan kapasitas teknis aparat penegak hukum dalam memahami forensik digital AI, menempatkan Indonesia dalam posisi yang sangat rentan terhadap eksploitasi data berbasis AI, khususnya oleh korporasi multinasional atau pelaku

[23] Singapore Parliament, Ministerial Statement on the Regulation of Artificial Intelligence in Singapore (Singapore: Ministry of Communications and Information, 2023). Singapura mengadopsi National AI Strategy 2.0 dengan pendekatan regulasi yang lebih fleksibel dan berbasis industri dibanding EU AI Act.

[24] Parmena Olimid, A. Legal Analysis Of Eu Artificial Intelligence Act (2024): Insights From Personal Data Governance And Health Policy. Access to Justice in Eastern Europe.

[25] Ridzuan, N.N., Masri, M., Anshari, M., Fitriyani, N., & Syafrudin, M. AI in the Financial Sector: The Line between Innovation, Regulation and Ethical Responsibility. Inf., 15, (2024), hlm. 432.

Creative Commons Attribution 4.0 International License

kejahatan siber lintas batas.[26]

Dari perspektif korban, sistem UE menyediakan perlindungan paling komprehensif hak atas ganti rugi (Pasal 82 GDPR), hak atas penghapusan *data right to be forgotten*, hak atas portabilitas data, dan hak untuk tidak tunduk pada keputusan otomatis sepenuhnya. Mekanisme *class action* melalui organisasi masyarakat sipil (Pasal 80 GDPR) memungkinkan penggugatan kolektif yang efektif.[27] Indonesia, dalam UU PDP, memang mengatur hak-hak subjek data (Pasal 5-16) yang sebagian besar mengacu pada GDPR, namun hak-hak tersebut sebagian besar bersifat deklaratif tanpa mekanisme *enforcement* yang jelas. Tidak ada ketentuan tentang *representative action* yang memungkinkan LSM mengajukan gugatan atas nama subjek data, dan prosedur pengaduan kepada Lembaga PDP belum diatur secara rinci.[28] Akibatnya, subjek data yang dirugikan oleh sistem AI dalam konteks Indonesia praktis tidak memiliki jalur hukum yang efektif dan terjangkau untuk memperoleh keadilan.

Studi komparatif ini membawa pada simpulan yang tegas: Indonesia membutuhkan rekonstruksi hukum pidana yang tidak sekadar bersifat tambalan (*patchwork regulation*), melainkan sebuah arsitektur regulasi AI yang bersifat komprehensif, sistemik, dan berorientasi pada hak. Model UE relevan sebagai inspirasi utama mengingat konvergensi sistem hukum, sementara model Singapura dapat diadopsi untuk aspek-aspek yang memerlukan fleksibilitas dan pragmatisme industri.

E. Penutup

Berdasarkan analisis yang telah dilakukan, penelitian ini menarik dua kesimpulan utama sebagai jawaban atas rumusan masalah yang diajukan. Pertama, konstruksi pertanggungjawaban pidana atas pelanggaran data pribadi berbasis AI dalam hukum pidana positif Indonesia bersifat fragmentaris dan inkomplit. Rezim pidana yang ada tersebar dalam UU PDP, UU ITE, dan KUHP Baru mengandung tiga kekosongan hukum kritis ketiadaan definisi sistem AI yang dapat dijadikan basis konstruksi delik; ambiguitas dalam pembuktian *mens rea* ketika *actus reus* dilakukan oleh algoritma otonom; dan ketiadaan mekanisme *strict liability* korporasi yang eksplisit. Ketiga kekosongan ini secara kolektif menciptakan 'zona impunitas' bagi pengembang dan operator AI yang mengeksploitasi data pribadi dalam skala masif. Meskipun KUHP Baru telah memperbarui doktrin pertanggungjawaban korporasi, belum ada jembatan konseptual yang menghubungkan doktrin tersebut secara eksplisit dengan konteks kejahatan berbasis AI. Kedua, perbandingan dengan Uni Eropa dan Singapura menunjukkan bahwa Indonesia secara struktural tertinggal dalam hal *legislative completeness*, *institutional capacity*, dan *victim protection mechanisms*. Uni Eropa unggul dalam *comprehensiveness* dan *preventive orientation* melalui integrasi GDPR-AI Act, sedangkan Singapura unggul dalam *regulatory agility* melalui model tata kelola berbasis akuntabilitas. Indonesia perlu mengadopsi pendekatan hibrida: mengambil prinsip *by-design accountability* dari UE untuk norma pidana substantif, serta pragmatisme pengaturan berbasis risiko dari

[26] Praja, B. A. "Hukum Perlindungan Data Pribadidi Era Kecerdasan Buatan (Ai)". Journal of Law and Social Change Review, 1(01), 2026

[27] Şerban, A. The legal framework of data subject representation. SHS Web of Conferences. 2023

[28] Jannah, M., Amboro, F.Y., & Shahrullah, R.S. Personal Data Protection in Telemedicine: Comparison of Indonesian and European Union Law. Journal of Law and Policy Transformation., (2024)

Creative Commons Attribution 4.0 International License

Singapura untuk implementasinya. Tanpa rekonstruksi yang sistemik, Indonesia berpotensi menjadi '*data exploitation haven*' bagi aktor teknologi yang berupaya menghindari regulasi ketat di yurisdiksi lain.

Daftar Pustaka

Articles, Books, adn Reports

Auliya, S.F., Kudina, O., Ding, A.Y., & van de Poel, I. AI versus AI for democracy: exploring the potential of adversarial machine learning to enhance privacy and deliberative decision-making in elections. *AI and Ethics*, 5, (2024): 2801 - 2813.

Balkin, Jack M. The Three Laws of Robotics in the Age of Big Data. *Ohio State Law Journal*, 78(5), (2017): 1217-1241

Dvornikova, P., & Osadchaya, A. Artificial Intelligence And The Law: The Challenges Of Establishing Criminal Liability In The Digital Age. *Juridical scientific and electronic journal*, 2024.

Eurike Hailtik, A.G., & Afifah, W. Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia. *Asian Journal of Social and Humanities*, 2024.

Ginting, Y. Akuntabilitas Pidana di Era Penyalahgunaan Kecerdasan Buatan ditinjau dari Asas Legalitas. *The Prosecutor Law Review*, 3(3), 2025

Hutchinson, T.. *Doctrinal legal research: Focus on method*. Dalam M. McConville & W. H. Chui (Eds.), *Research methods for law*. Edinburgh University Press, 2017: 7-33

Jannah, M., Amboro, F.Y., & Shahrullah, R.S. Personal Data Protection in Telemedicine: Comparison of Indonesian and European Union Law. *Journal of Law and Policy Transformation*, 2024

Lim, S.S., & Chng, G. Verifying AI: will Singapore's experiment with AI governance set the benchmark? *Communication Research and Practice*, 10, 2024: 297 - 306.

Pamungkas, A. A., Sutarni, N., & Pranawa, B. Legal analysis of deepfake technology in Indonesia from the perspective of fair and civilized humanity. *Pena Justisia: Media Komunikasi Dan Kajian Hukum*, 24(1), 2025: 4562-4574

Parmena Olimid, A. (2024). *Legal Analysis Of Eu Artificial Intelligence Act (2024): Insights From Personal Data Governance And Health Policy*. Access to Justice in Eastern Europe.

Praja, B. A. Hukum Perlindungan Data Pribadidi Era Kecerdasan Buatan (Ai). *Journal of Law and Social Change Review*, 1(01), 2026

Rahmah, A. P. A., Anggraini, P. O., & Hasbi, M. Perlindungan Data Pribadi Sebagai Hak Asasi Manusia di Era Digital: Analisis dan Perbandingan Indonesia dan Singapura. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 4(3), (2026): 3242-3249.

Ridzuan, N.N., Masri, M., Anshari, M., Fitriyani, N., & Syafrudin, M. AI in the *Financial Sector: The Line between Innovation, Regulation and Ethical Responsibility*. Inf., 15, (2024): 432.

Sayyed, H. Artificial intelligence and criminal liability in India: exploring legal implications and challenges. *Cogent Social Sciences*, 10, (2024)

Singapore Parliament, *Ministerial Statement on the Regulation of Artificial Intelligence in Singapore* (Singapore: Ministry of Communications and Information, 2023).

Soekanto, S., & Mamudji, S.. *Penelitian hukum normatif: Suatu tinjauan singkat* (Cet.

Creative Commons Attribution 4.0 International License

13). Rajawali Pers.(2011)

Legal Regulations and Decisions

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation/GDPR), OJ L 119, 4.5.2016.

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

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana diubah oleh Undang-Undang Nomor 19 Tahun 2016.

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

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

Government Sources, News, and Empirical Data

Anggie Irfansyah, Ketika AI Berhadapan dengan Hukum:Apa yang Harus Diketahui Bisnis Indonesia Sebelum Terlambat, Inixindo Jogja, 2026

Divino, S.B. (2020). Critical considerations on Artificial Intelligence liability: e-personality propositions.

Republic of Singapore. (2012). Personal Data Protection Act 2012 (No. 26 of 2012), sebagaimana diubah oleh Personal Data Protection (Amendment) Act 2020.

Şerban, A. (2023). The legal framework of data subject representation. SHS Web of Conferences.

Creative Commons Attribution 4.0 International License