JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik
E-ISSN: 2747-1993
P-ISSN: 2747-2000
https://dinastirev.org/JIHHP dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jihhp.v6i4

Perlindungan Hukum terhadap *Inferred data* dalam Automated Decision-Making: Studi Perbandingan GDPR dan UU PDP

Adela Oktaviani Putri[1], Sekar Dwiyanti[2], Nur Azmi Azis[3].
[1]Universitas Airlangga, Surabaya, Indonesia, adela.oktaviani.putri-2024@fh.unair.ac.id
[2]Universitas Airlangga, Surabaya, Indonesia, sekar.dwiyanti-2024@fh.unair.ac.id.
[3]Universitas Airlangga, Surabaya, Indonesia, nur.azmi.azis-2024@fh.unair.ac.id

Corresponding Author: adela.oktaviani.putri-2024@fh.unair.ac.id

Abstract: *The rapid advancement of artificial intelligence technologies and automated decision-making (ADM) systems has given rise to data inference practices capable of generating individual profiles without the direct involvement of data subjects. The use of inferred data within ADM systems poses serious risks to individual rights, including the potential for algorithmic discrimination, privacy violations, and a lack of transparency in automated decisions. This study examines two principal issues: first, how the General Data Protection Regulation (GDPR) classifies inferred data as personal data in the context of profilingand ADM; and second, how the Indonesian Personal Data Protection Law (UU PDP) regulates the protection against risks posed by inferred data in ADM. This study employs a normative legal research method, utilizing a statute approach and a conceptual approach. The findings indicate that the GDPR classifies inferred data as part of personal data through the broad definition set forth in Article 4(1) and situates it within the regulatory framework governing profilingand ADM under Article 4(4) and Article 22, accompanied by a comprehensive set of data subject rights. By contrast, the UU PDP does not explicitly regulate inferred data , addressing it instead through a functional approach derived from the definition of personal data under Article 1(1), processing principles, data subject rights, and controller obligations. Nevertheless, a significant normative gap remains in comparison to the GDPR's standard of protection, necessitating regulatory reinforcement through more specific implementing regulations.*

Keyword: *Inferred data , Personal Data Protection, GDPR, UU PDP, Automated Decision-Making*

Abstrak: Perkembangan kecerdasan buatan dan sistem *automated decision-making* (ADM) mendorong penggunaan *inferred data* yang memungkinkan pembentukan profil individu tanpa keterlibatan langsung subjek data. Praktik ini menimbulkan risiko terhadap hak individu, termasuk diskriminasi algoritmik dan kurangnya transparansi. Namun, belum ada kajian yang secara spesifik membandingkan perlindungan *inferred data* dalam kedua rezim ini. Penelitian ini bertujuan menganalisis klasifikasi *inferred data* dalam kerangka GDPR serta menilai

pengaturan perlindungannya dalam Undang-Undang Pelindungan Data Pribadi (UU PDP). Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual. Hasil penelitian menunjukkan bahwa GDPR mengklasifikasikan *inferred data* sebagai data pribadi melalui definisi luas serta mengaturnya dalam rezim *profiling*dan ADM yang disertai perlindungan hak subjek data yang komprehensif. Sebaliknya, UU PDP belum mengatur *inferred data* secara eksplisit dan masih bergantung pada pendekatan umum, sehingga menimbulkan kesenjangan normatif dalam perlindungan terhadap risiko yang timbul dari ADM. Penelitian ini menegaskan perlunya penguatan pengaturan *inferred data* dalam UU PDP guna menjamin kepastian dan efektivitas perlindungan hukum.

Kata Kunci: *Inferred data* , Perlindungan Data Pribadi, GDPR, UU PDP, *Automated Decision-Making*

.

PENDAHULUAN

Perkembangan teknologi di era digital membawa banyak dampak yang ikut mengubah pola kehidupan manusia baik secara positif maupun negatif. Salah satu bentuk akibat adanya perkembangan teknologi yakni munculnya kecerdasan buatan yang disebut sebagai *artificial intelligence* atau AI. Kecerdasan buatan (AI) kini banyak dimanfaatkan di berbagai bidang, seperti kesehatan, transportasi, dan pendidikan(Barn, 2020). Tujuannya adalah meningkatkan produktivitas, efisiensi, serta kualitas hidup manusia. AI memiliki kemampuan yang meniru kecerdasan manusia, misalnya dalam memecahkan masalah, belajar hal baru, dan mengambil keputusan. Teknologi ini juga memungkinkan pemrosesan data dalam skala besar dengan kecepatan tinggi, sehingga mendukung pengambilan keputusan yang sebelumnya dilakukan secara manual(Li et al., 2025). Keberadaan AI saat ini telah mempengaruhi lapangan pekerjaan dengan menggantikan pekerjaan manusia, termasuk berpindahnya kewenangan pengambilan keputusan dari manusia ke algoritma dalam sistem yang dikenal sebagai *automated decision-making* (ADM) (Choroszewicz, 2026).

Dalam praktik ADM, sistem algoritmik tidak hanya memproses data yang secara langsung diberikan oleh individu, tetapi juga menghasilkan kategori data baru melalui mekanisme *profiling* dan pemrosesan otomatis sebagaimana dimaksud dalam Pasal 4 (4) GDPR. Kategori data tersebut dikenal dalam literatur sebagai *inferred data* , yakni data yang dihasilkan melalui proses inferensi atau penarikan kesimpulan berdasarkan data lain yang telah tersedia. Berbeda dengan *observed data* yang diperoleh melalui pengamatan langsung terhadap aktivitas individu (Parluhutan, 2021), *inferred data* merupakan hasil pemrosesan lanjutan yang bersifat prediktif dan dibentuk oleh algoritma yang dapat mengandung bias dan kesalahan. Misalnya, pola penggunaan media sosial dapat digunakan untuk memprediksi orientasi politik, stabilitas emosional, tingkat stres, kecenderungan religius, atau kelayakan kredit seseorang (Dham et al., 2021). Melalui *profiling*, sistem algoritmik menghubungkan berbagai variabel data untuk menghasilkan kesimpulan mengenai individu yang kemudian menjadi dasar dalam sistem ADM, baik berupa persetujuan, penolakan, maupun perlakuan tertentu dalam konteks penilaian kelayakan kredit, rekrutmen tenaga kerja, prediksi risiko kesehatan, serta penyajian konten yang dipersonalisasi (Wiedemann, 2022).

Penggunaan *inferred data* dalam *profiling* dan ADM menimbulkan berbagai risiko hukum yang signifikan. Risiko tersebut meliputi potensi hasil keputusan yang diskriminatif, kurangnya transparansi terhadap dasar pengambilan keputusan, serta potensi pelanggaran hak atas privasi dan perlindungan data pribadi karena keputusan penting diambil tanpa partisipasi atau pemahaman subjek data (Wahyuningtyas, 2024). Risiko tersebut semakin diperkuat oleh keterbatasan kemampuan subjek data untuk memahami, mengakses, atau menantang *inferred data* yang digunakan untuk menilai dirinya. Hubungan antara profiling, *inferred data* , dan

ADM menunjukkan bahwa *inferred data* tidak hanya bersifat informasional, tetapi juga memiliki fungsi normatif yang secara langsung mempengaruhi posisi hukum dan sosial individu. Oleh karena itu, regulasi perlindungan data dituntut untuk tidak hanya berfokus pada data yang diamati atau diberikan secara langsung, tetapi juga mencakup data hasil inferensi yang dihasilkan melalui proses *profiling* dan pemrosesan otomatis.

Dalam konteks global, *General Data Protection Regulation* (GDPR) Uni Eropa sering dipandang sebagai tolok ukur utama dalam pengaturan perlindungan data pribadi. GDPR dikenal sebagai rezim perlindungan data yang komprehensif dan berpengaruh, dengan dampak ekstrateritorial yang luas terhadap praktik regulasi di berbagai negara melalui fenomena yang dikenal sebagai *Brussels Effect* (Tamim, 2024). GDPR mengadopsi definisi data pribadi yang luas, memberikan pengaturan eksplisit mengenai *profiling*, serta menetapkan perlindungan khusus terhadap pengambilan keputusan otomatis yang berdampak signifikan terhadap individu. Meskipun demikian, GDPR tidak secara eksplisit mendefinisikan atau mengatur *inferred data* sebagai kategori data tersendiri (Häuselmann & Custers, 2024). Ketentuan-ketentuan yang ada mengatur *profiling* dan pengambilan keputusan otomatis, tetapi tidak secara tegas menjawab bagaimana *inferred data* harus diklasifikasikan dan dilindungi dalam seluruh siklus pemrosesan data. Ketidakjelasan ini menunjukkan bahwa status hukum *inferred data* dalam kerangka GDPR masih bersifat ambigu dan bergantung pada interpretasi yurisprudensi, sehingga belum terdapat kepastian hukum yang memadai bagi subjek data maupun pengendali data. Dalam konteks nasional, Indonesia telah mengalami perkembangan signifikan dalam hukum perlindungan data pribadi dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Dalam proses pembentukannya, UU PDP mengadopsi prinsip-prinsip hukum umum dan praktik internasional, termasuk GDPR dari Uni Eropa (Pradana & Saragih, 2024). Namun demikian, UU PDP belum secara eksplisit mengatur *inferred data* sebagai kategori data tersendiri dan pengaturan mengenai ADM masih bersifat umum, sehingga berpotensi menimbulkan celah perlindungan bagi subjek data ketika keputusan berbasis ADM menghasilkan dampak yang merugikan hak-hak individu.

Sejumlah penelitian terdahulu telah menyoroti problematika *inferred data* , namun masih menyisakan celah kajian yang signifikan. Jurnal berjudul *"Tell me something new: data subject rights applied to inferred data and profiles"* menekankan bahwa *inferred data* tidak diatur sebagai kategori tersendiri, namun tetap dapat dianggap sebagai data pribadi bila memenuhi unsur definisi GDPR. Kajian lain berjudul *"Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR"* menyoroti ambiguitas penerapan Pasal 22 GDPR dalam konteks *profiling*dan ADM. Sementara itu, kajian di Indonesia masih terbatas pada analisis umum UU PDP, seperti penelitian berjudul *"Perlindungan Hak Subjek Data dalam Transfer Data Pribadi: Analisis Perbandingan UU PDP dengan GDPR"* yang membandingkan kedua regulasi tersebut tanpa secara khusus membahas risiko *inferred data* dalam sistem ADM. Dengan demikian, terdapat kekosongan kajian yang belum terjawab mengenai bagaimana *inferred data* diklasifikasikan dan dilindungi secara komparatif dalam kerangka GDPR dan UU PDP, khususnya dalam konteks ADM.

Berdasarkan uraian di atas, penelitian ini bertujuan mengisi kekosongan tersebut dengan mengkaji perlindungan hukum terhadap *inferred data* dalam sistem ADM melalui studi perbandingan antara GDPR dan UU PDP. Secara spesifik, penelitian ini merumuskan dua pertanyaan utama: pertama, bagaimana GDPR mengklasifikasikan *inferred data* dalam konteks *profiling*dan pengambilan keputusan otomatis; dan kedua, bagaimana UU PDP mengatur perlindungan terhadap risiko *inferred data* akdalam sistem ADM.

METODE

Penelitian ini merupakan penelitian hukum normatif yang berfokus pada analisis pengaturan *inferred data* dalam rezim perlindungan data, khususnya dalam konteks *profiling*dan *automated decision-making* (ADM). Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), serta pendekatan komparatif (*comparative approach*) untuk membandingkan pengaturan antara GDPR dan Undang-Undang Pelindungan Data Pribadi (UU PDP). Adapun bahan hukum yang digunakan terdiri atas bahan hukum primer berupa peraturan perundang-undangan, khususnya GDPR dan UU PDP, serta bahan hukum sekunder berupa buku, artikel jurnal, dan doktrin hukum yang relevan dengan isu *inferred data* , *profiling*, dan ADM. Bahan hukum dipilih berdasarkan relevansinya terhadap topik *inferred data* dan sistem pengambilan keputusan otomatis dalam yurisdiksi Uni Eropa dan Indonesia.Teknik analisis bahan hukum dilakukan secara deskriptif-analitis. Analisis ini digunakan untuk mengidentifikasi dan menguraikan konsep serta norma hukum terkait *inferred data* dalam masing-masing rezim. Selanjutnya, dilakukan analisis komparatif untuk membandingkan pengaturan dalam GDPR dan UU PDP guna menemukan persamaan, perbedaan, serta tingkat perlindungan yang diberikan, sekaligus mengidentifikasi adanya kesenjangan pengaturan dalam konteks perlindungan terhadap risiko *inferred data* dalam ADM.

HASIL DAN PEMBAHASAN

A). Klasifikasi Hukum *Inferred data* dalam Kerangka GDPR

1) Kategorisasi Data Pribadi dan Status Hukum *Inferred data* Menurut GDPR

Menurut Pasal 4 ayat (1) GDPR, data pribadi mencakup seluruh informasi yang dapat mengidentifikasi seseorang, baik melalui nama, nomor identifikasi kependudukan, data lokasi, maupun karakteristik fisik atau genetik, termasuk data yang diperoleh melalui telepon, kartu kredit, nomor personel, akun, plat nomor kendaraan, penampilan fisik, nomor pelanggan, atau alamat (Pradana & Saragih, 2024). Berdasarkan pedoman yang diterbitkan oleh Article 29 Data Protection Working Party, data pribadi dapat dibedakan berdasarkan sumber perolehannya menjadi empat jenis, yaitu: *provided data, observed data, derived data,* dan *inferred data* (*Guidelines on the Right to Data Portability*, 2017).

Provided data merupakan data yang diberikan secara langsung dan sukarela oleh individu kepada perusahaan atau penyedia layanan, seperti identitas pribadi, data kontak, dan informasi akun, sehingga dalam kategori ini terdapat unsur kesadaran serta persetujuan individu yang memungkinkan peredaran data lebih mudah dikendalikan melalui mekanisme *privacy consent* (Wachter & Mittelstadt, 2019). Observed data merupakan data yang diperoleh secara pasif dari aktivitas atau perilaku individu, seperti riwayat penjelajahan (browsing history) maupun pola interaksi di media sosial, yang terekam secara otomatis oleh sistem tanpa keterlibatan langsung dari individu, sehingga individu sering kali tidak menyadari sejauh mana data mereka terkumpul dan meningkatkan risiko penyalahgunaan (Kosinski et al., 2013). Derived data adalah data baru yang muncul dari proses perhitungan atau klasifikasi atas data yang sudah ada, misalnya rasio utang terhadap pendapatan atau rata-rata belanja per kunjungan, yang bersifat faktual karena tidak mengandung unsur prediksi maupun interpretasi perilaku individu (Abrams, 2014).

Berbeda dari ketiga kategori tersebut, inferred data adalah data yang dihasilkan melalui proses analisis probabilistik atau prediktif, misalnya skor kredit, skor risiko penipuan, atau prediksi kemungkinan seseorang mengidap penyakit tertentu, yang sepenuhnya lahir dari proses analitik kompleks tanpa keterlibatan individu dalam penciptaannya, sehingga individu pada umumnya tidak menyadari keberadaan data

ini(Abrams, 2014). Ciri utama *inferred data* terletak pada sifatnya yang berbasis prediksi dan korelasi: tidak diberikan oleh individu baik secara langsung maupun tidak langsung, melainkan dikonstruksi oleh sistem berdasarkan kebiasaan dan aktivitas individu. Sebagai contoh, pola pencarian produk bayi di aplikasi belanja daring dapat digunakan untuk memprediksi bahwa individu tersebut sedang mempersiapkan kelahiran anak, meskipun prediksi tersebut tidak selalu akurat dan tidak diketahui oleh pengguna (Matsumi & Solove, 2024).

Perbedaan antara derived data dan *inferred data* penting untuk ditegaskan: derived data merupakan turunan langsung dari data yang sudah ada dan bersifat faktual, sedangkan inferred *data* bersifat prediktif dengan memperkirakan sesuatu yang belum tentu akurat tentang individu. Hal ini menjadikan *inferred data* sebagai kategori data pribadi yang paling problematis dalam konteks hukum perlindungan data, karena dampaknya terhadap hak dan kepentingan subjek data seringkali lebih signifikan dibandingkan data yang bersifat faktual. Oleh karena itu, analisis mengenai kedudukan hukum *inferred data* tidak dapat disamakan dengan kategori data pribadi lainnya, melainkan harus ditempatkan dalam kerangka pengaturan yang mempertimbangkan risiko, ketidakseimbangan informasi, serta implikasinya terhadap praktik *profiling*dan ADM.

2) Hubungan *Inferred data* , *Profiling*, dan ADM dalam Kerangka GDPR

Karakteristik *inferred data* yang bersifat prediktif menimbulkan tantangan serius terhadap prinsip-prinsip fundamental perlindungan data. Prinsip *lawfulness* dan *fairness* sering kali terhambat karena proses inferensi terjadi tanpa keterlibatan aktif subjek data dan tanpa dasar persetujuan yang jelas. Prinsip *transparency* sulit dipenuhi karena pemodelan AI cenderung kompleks dan bahkan terkadang sulit dijelaskan secara teknis oleh pengendali data itu sendiri. Sementara itu, prinsip accountability menjadi problematis karena hubungan antara data input dan hasil inferensi sering kali kabur dan tidak mudah ditelusuri. Hal ini menunjukkan bahwa inferred data secara inheren bertensi dengan prinsip-prinsip dasar GDPR, dan implikasinya adalah diperlukannya pengaturan yang lebih spesifik untuk menjembatani kesenjangan tersebut.

Dalam kerangka GDPR, inferred data tidak berdiri sebagai norma mandiri, melainkan berkaitan erat dengan profilingdan ADM. Pasal 4(4) GDPR mengatur profiling sebagai bentuk pemrosesan data pribadi yang dilakukan secara otomatis untuk menilai aspek tertentu dari seseorang, termasuk prediksi dalam hal ekonomi, minat, perilaku, dan kesehatan. Namun demikian, tidak semua pengelompokan data secara otomatis dapat dikategorikan sebagai profiling; pengelompokan berdasarkan jenis kelamin atau usia, misalnya, tidak termasuk profiling jika tidak digunakan untuk menilai atau memprediksi aspek-aspek pribadi sebagaimana dimaksud dalam ketentuan tersebut (Wiedemann, 2022).

Hubungan antara inferred data dan profiling bersifat hierarkis. Inferred data merupakan potongan informasi yang dihasilkan dari data mentah, misalnya dari tanggal lahir dapat ditebak usia, atau dari data penghasilan dapat ditentukan skor kredit, sedangkan profiling memiliki cakupan yang lebih luas karena menggabungkan beberapa *inferred data* dengan data lainnya untuk membentuk profil tertentu tentang individu. Penggunaan *inferred data* dalam *profiling* secara berulang dapat menimbulkan akibat serius, seperti memposisikan individu dalam kategori yang sulit diubah, memperkuat bias algoritmik, dan menciptakan prediksi yang bersifat *self-fulfilling prophecy* yakni kondisi di mana sistem justru memperkuat kesimpulan yang dibuatnya sendiri.

Selanjutnya, *inferred data* dalam konteks ADM memiliki peran sentral karena ADM selalu bergantung pada hasil analisis sebelumnya (*profiling*). Tanpa *inferred data*

dari tahap *profiling*, sistem tidak memiliki dasar untuk membuat keputusan otomatis seperti perhitungan risiko, seleksi kandidat, atau penentuan kelayakan. ADM bekerja dengan alur berurutan yang dimulai dari data mentah, kemudian dilanjutkan dengan *profiling*, menghasilkan *inferred data* , yang selanjutnya diproses melalui model keputusan hingga menghasilkan *output* ADM. Implikasinya, keakuratan dan keadilan keputusan ADM secara langsung bergantung pada kualitas dan integritas inferred data yang dihasilkan pada tahap sebelumnya, sehingga kelemahan pada tahap inferensi akan berdampak sistemik terhadap seluruh rantai pengambilan keputusan (Holtz & Ledendal, 2026).

GDPR mengatur tiga bentuk penggunaan profiling: (1) profilingumum yang tidak menghasilkan keputusan; (2) pengambilan keputusan berbasis profil namun tetap melibatkan penilaian manusia; dan (3) pengambilan keputusan yang sepenuhnya otomatis dan menimbulkan dampak bagi individu (Party, 2018). Pasal 22(1) GDPR memberikan perlindungan agar seseorang tidak langsung dikenai keputusan yang sepenuhnya dibuat oleh sistem otomatis apabila keputusan tersebut membawa konsekuensi hukum atau berdampak nyata, dan perlindungan ini berlaku secara otomatis tanpa perlu diminta terlebih dahulu. Hal ini dipertegas dalam Recital 71 GDPR yang menyatakan bahwa keputusan otomatis berbasis profiling hanya boleh dilakukan dalam kondisi tertentu, yakni jika diperlukan untuk pelaksanaan kontrak, diizinkan oleh hukum, atau didasarkan pada persetujuan eksplisit subjek data, sehingga pemrosesan dalam lingkup Pasal 22(1) pada prinsipnya dilarang kecuali salah satu dari tiga pengecualian dalam Pasal 22(2) terpenuhi.

Pasal 9(1) GDPR mengatur larangan mutlak pemrosesan kategori khusus data pribadi, yang mencakup ras/etnis, keyakinan agama, pandangan politik, keanggotaan serikat pekerja, data genetik, data biometrik, data kesehatan, serta kehidupan seks dan orientasi seksual. Yang perlu dicermati secara kritis adalah bahwa *inferred data* dapat "menerobos" ke dalam kategori data sensitif ini meskipun data asalnya bersifat biasa. Sebagai contoh, data dari struk belanja, pola konsumsi, dan lokasi dapat digunakan untuk menarik kesimpulan mengenai kondisi kesehatan, orientasi seksual, atau pandangan politik seseorang. Hal ini menunjukkan bahwa batas antara data biasa dan data sensitif dalam era inferensi algoritmik menjadi semakin kabur, dan implikasinya adalah perlindungan Pasal 9 GDPR berpotensi menjadi tidak efektif apabila tidak dibarengi dengan pengaturan khusus mengenai *inferred data* itu sendiri.

3) Hak Subjek Data terhadap *Inferred data* dalam GDPR

Hak yang berhubungan dengan penggunaan *inferred data* dalam ADM diatur dalam berbagai pasal GDPR. Pasal 5(1)(a) GDPR mewajibkan pengendali data untuk memastikan subjek data tetap diberi informasi sesuai Pasal 13 dan 14 GDPR tentang bagaimana data pribadi mereka digunakan, sehingga memungkinkan individu menggunakan hak-hak mereka sebagaimana diatur dalam Pasal 15 hingga 22 GDPR (Party, 2018). Hak atas informasi ini merupakan instrumen utama untuk mengungkap sifat inferensi yang pada dasarnya tidak terlihat *(invisible)* bagi subjek data, sekaligus berfungsi sebagai safeguard sebagaimana ditegaskan dalam Recital 71 yang menuntut adanya penjelasan yang memungkinkan individu memahami dasar penilaian dan menantang keputusan otomatis (Wiedemann, 2022).

Pasal 15 GDPR memberikan hak akses kepada subjek data terhadap data yang digunakan dalam pembentukan profil, sekaligus untuk mengetahui output dari proses inferensi termasuk segmen atau kategori tempat mereka ditempatkan. Pasal 16, 17, 18, dan 21 GDPR selanjutnya mengatur hak untuk memperbaiki ketidakakuratan dalam data input maupun output inferensi, hak penghapusan data tertentu, pembatasan pemrosesan, serta pengajuan keberatan terhadap *profiling*. Dalam hal ini, hak

mengajukan keberatan berlaku secara absolut dalam konteks pemasaran langsung termasuk *profiling* untuk tujuan tersebut sebagaimana ditegaskan dalam Pasal 21(2) GDPR.

Secara kritis, meskipun GDPR menyediakan kerangka hak yang relatif komprehensif, efektivitasnya terhadap *inferred data* masih mengandung kelemahan struktural. Pertama, tidak adanya definisi eksplisit *inferred data* dalam GDPR menciptakan ambiguitas mengenai apakah dan sejauh mana hak-hak tersebut dapat diterapkan terhadap data hasil inferensi (Häuselmann & Custers, 2024). Kedua, hak akses terhadap *inferred data* dalam praktiknya sulit diimplementasikan karena kompleksitas algoritma membuat penjelasan yang bermakna (*meaningful explanation*) kepada subjek data menjadi tantangan tersendiri. Implikasinya, celah antara pengaturan normatif dan implementasi praktis GDPR terhadap *inferred data* masih signifikan dan memerlukan perkembangan yurisprudensi lebih lanjut.

B). Pengaturan Perlindungan Subjek Data terhadap Risiko *Inferred data* dalam UU PDP Indonesia

1) Kualifikasi *Inferred data* sebagai Data Pribadi dalam UU PDP

Pasal 1 angka 1 UU PDP mendefinisikan data pribadi sebagai "data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik." Definisi ini secara fungsional bersifat luas karena perlindungan tidak hanya terbatas pada data yang secara langsung mengidentifikasi seseorang, tetapi juga mencakup data yang apabila dikombinasikan dengan informasi lain dapat mengidentifikasi individu tertentu.

Meskipun UU PDP tidak secara eksplisit mendefinisikan inferred data sebagai kategori tersendiri, pendekatan fungsional dapat digunakan untuk menilai substansi serta karakteristiknya, termasuk bagaimana praktik penggunaannya dan tujuan pengolahannya (Attamongkol & Putra, 2025). Berdasarkan Pasal 1 angka 1 UU PDP, sepanjang data hasil inferensi dapat diidentifikasi terkait dengan individu tertentu, baik secara tersendiri maupun dikombinasi dengan informasi lain, maka data tersebut memenuhi kriteria sebagai data pribadi dan tunduk pada ketentuan perlindungan UU PDP. Hal ini menunjukkan bahwa perlindungan terhadap *inferred data* dalam UU PDP bersifat implisit dan bergantung sepenuhnya pada interpretasi definitif, yang implikasinya menciptakan ketidakpastian hukum bagi pengendali data maupun subjek data dalam praktik penerapannya.

Relevansi *inferred data* dalam sistem pemrosesan modern tidak dapat diabaikan, karena data hasil inferensi telah menjadi komponen krusial dalam berbagai aplikasi teknologi kontemporer, mulai dari sistem rekomendasi, credit scoring, hingga targeted advertising, dengan nilai strategisnya yang terletak pada kemampuannya mengungkap aspek tentang individu yang tidak pernah secara eksplisit diungkapkan, seperti kondisi kesehatan mental (Custers & Vrabec, 2024). Kondisi ini mempertegas urgensi pengaturan yang lebih eksplisit terhadap *inferred data* dalam kerangka UU PDP, mengingat dampak penggunaannya yang semakin masif dalam berbagai keputusan yang bersifat signifikan bagi kehidupan individu.

2) Risiko *Inferred data* dalam Sistem ADM dan Respons UU PDP

ADM dalam konteks UU PDP dapat dipahami sebagai proses pengambilan keputusan yang dilakukan secara otomatis oleh sistem elektronik dengan menggunakan algoritma, model prediktif, dan kecerdasan buatan untuk memproses data pribadi dan menghasilkan keputusan yang berdampak signifikan terhadap individu.(Wahyuningtyas, 2024) Penggunaan *inferred data* dalam sistem ADM menimbulkan setidaknya tiga risiko khusus yang perlu dicermati secara kritis.

Pertama, risiko bias algoritmik terjadi ketika data historis yang digunakan untuk melatih sistem mengandung bias tertentu, sehingga menghasilkan inferensi yang diskriminatif dan berdampak sistemik terhadap kelompok-kelompok tertentu (Wahyuningtyas, 2024). Kedua, risiko kesalahan prediksi yang inheren dalam setiap model inferensi, mengingat tidak ada sistem prediksi yang sempurna, dan kesalahan tersebut dapat berdampak langsung merugikan individu yang bersangkutan, terutama dalam konteks keputusan bernilai tinggi seperti pemberian kredit atau rekrutmen kerja. Ketiga, risiko diskriminasi dapat muncul ketika inferensi digunakan untuk mengategorikan individu secara berbeda berdasarkan karakteristik yang disimpulkan, bukan fakta yang terverifikasi, termasuk prediksi atas karakteristik sensitif seperti orientasi seksual, kondisi kesehatan mental, atau kemungkinan terkena penyakit tertentu di masa mendatang, yang bahkan mungkin tidak diketahui oleh individu itu sendiri (Custers & Vrabec, 2024). Implikasinya bagi Indonesia adalah bahwa penggunaan ADM berbasis inferred data yang tidak diawasi secara ketat berpotensi menimbulkan pelanggaran hak-hak individu yang bersifat masif namun sulit dideteksi oleh korbannya sendiri.

Merespons risiko-risiko tersebut, UU PDP tidak menggunakan terminologi yang spesifik seperti halnya GDPR, namun ketentuan terkait pemrosesan otomatis dapat ditemukan secara implisit dalam berbagai pasal yang mengatur pemrosesan data pribadi secara umum, khususnya dalam konteks hak subjek data untuk menolak atau mengajukan keberatan terhadap keputusan yang dihasilkan melalui pemrosesan otomatis. Dalam mengatur ADM dan profiling, UU PDP mengadopsi pendekatan berbasis risiko *(risk-based approach)* yang tercermin dalam kewajiban pengendali data untuk melaksanakan Penilaian Dampak Perlindungan Data Pribadi (PDPD/DPIA) sebagaimana diatur dalam Pasal 34 UU PDP, bilamana pemrosesan data memiliki potensi risiko tinggi terhadap subjek data.

3) Prinsip-Prinsip Pemrosesan dan Hak Subjek Data dalam UU PDP

UU PDP menetapkan delapan prinsip dasar pemrosesan data pribadi sebagaimana diatur dalam Pasal 16 ayat (2), yang mencakup pengumpulan, pemrosesan, penyimpanan, dan penghapusan data secara legal dan transparan (Pradana & Saragih, 2024). Dalam konteks inferred data, beberapa prinsip memiliki relevansi yang sangat kritis.

Prinsip keabsahan, keadilan, dan transparansi (lawfulness, fairness, and transparency) mensyaratkan bahwa setiap pemrosesan data pribadi harus dilakukan atas dasar hukum yang jelas, tidak merugikan subjek data, dan dilaksanakan secara terbuka. Prinsip pembatasan tujuan mensyaratkan bahwa tujuan pemrosesan harus ditentukan secara spesifik sejak awal dan dijelaskan sebelum data pribadi dikumpulkan; hal ini menjadi sangat kritis dalam konteks *inferred data* karena data yang dihasilkan melalui proses inferensi sering kali melampaui ruang lingkup data yang secara eksplisit diberikan oleh subjek data, sehingga berpotensi melanggar kedua prinsip tersebut apabila tidak dikelola dengan kerangka hukum yang ketat (Andini, 2026). Prinsip keakuratan dan proporsionalitas sebagaimana diatur dalam Pasal 30 dan Pasal 28 UU PDP sangat krusial mengingat *inferred data* rentan terhadap ketidakakuratan, sehingga pengendali data harus memastikan model dan algoritma yang digunakan telah divalidasi dan dapat menghasilkan inferensi yang akurat (Pradana & Saragih, 2024).

Prinsip keamanan data sebagaimana diatur dalam Pasal 35 UU PDP mengharuskan perlindungan dari pengaksesan, pengungkapan, pengubahan, atau penyalahgunaan yang tidak sah, yang sangat relevan mengingat *inferred data* sering kali bersifat sensitive (Pradana & Saragih, 2024). Prinsip akuntabilitas dalam Pasal 47 UU PDP mewajibkan pengendali data untuk bertanggung jawab atas pemrosesan dan

menunjukkan pertanggungjawaban dalam pemenuhan kewajiban perlindungan data. Hal ini menuntut pengendali data untuk mampu menjelaskan logika, metode, dan algoritma yang digunakan dalam menghasilkan *inferred data* beserta dampak potensialnya, suatu tuntutan yang dalam prakteknya sangat menantang mengingat kompleksitas sistem AI yang digunakan.

UU PDP juga memberikan sejumlah hak kepada subjek data sebagaimana termuat dalam Pasal 5 sampai dengan Pasal 15 yang berfungsi sebagai mekanisme perlindungan terhadap risiko *inferred data* dalam ADM. Hak atas informasi (Pasal 5) memberikan dasar bagi subjek data untuk mengetahui bagaimana data mereka akan diproses, termasuk apakah digunakan untuk menghasilkan inferred data atau dalam sistem ADM. Hak perbaikan dan hak akses (Pasal 6 dan 7) memberikan hak untuk mendapatkan salinan data pribadi sekaligus melakukan pembaruan atas data yang tidak akurat; namun dalam konteks inferred data , implementasi hak ini menghadapi tantangan tersendiri karena UU PDP belum memberikan jawaban eksplisit mengenai apakah hak akses dan perbaikan tersebut mencakup inferred data yang dihasilkan tentang mereka.

Hak penghapusan data (Pasal 43-45 UU PDP) memberikan mekanisme bagi subjek data untuk menuntut penghapusan data hasil inferensi yang tidak lagi relevan atau yang diproses tanpa dasar hukum yang sah, meskipun hak ini tidak bersifat mutlak karena harus mempertimbangkan ketentuan perundang-undangan lain yang berlaku (Agustina & Wiraguna, 2025). Pasal 10 UU PDP memberikan hak kepada subjek data untuk mengajukan keberatan terhadap keputusan yang diambil semata-mata berdasarkan pemrosesan otomatis, termasuk profiling, yang menghasilkan konsekuensi hukum atau secara signifikan mempengaruhi subjek data. Namun yang perlu dikritisi adalah UU PDP tidak mendefinisikan lebih lanjut ambang batas "dampak signifikan" yang dimaksud, sehingga terdapat ruang ketidakpastian normatif yang membedakannya dari pengaturan GDPR yang lebih terperinci.

4) Perbandingan GDPR dan UU PDP dalam Perlindungan *Inferred data*

Berdasarkan uraian di atas, perbandingan antara GDPR dan UU PDP dalam mengatur perlindungan *inferred data* dapat disajikan dalam tabel berikut:

Tabel 1. perbandingan antara GDPR dan UU PDP dalam mengatur perlindungan *inferred data*

Aspek	GDPR (Uni Eropa)	UU PDP (Indonesia)
A. Definisi dan Klasifikasi Data Pribadi		
Definisi data pribadi	Pasal 4(1): semua informasi yang berkaitan dengan orang yang teridentifikasi atau dapat diidentifikasi, mencakup nama, nomor identifikasi, data lokasi, identifikasi daring, dan faktor fisik, fisiologis, genetik, mental, ekonomi, budaya, atau sosial.	Pasal 1 angka 1: data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.
Tipologi data pribadi	Article 29 WP mengakui empat tipologi: provided data, observed data, derived data, dan *inferred data* sebagai kategorisasi berbasis sumber perolehan data.	Pasal 4: membedakan data pribadi umum dan data pribadi spesifik (sensitif), tanpa kategorisasi berbasis sumber perolehan. Tidak mengenal tipologi provided/observed/derived/inferred secara eksplisit.

Pengakuan *inferred data*	Tidak didefinisikan secara eksplisit, namun diakui melalui pedoman Article 29 WP dan yurisprudensi sebagai bagian dari data pribadi sepanjang memenuhi unsur identifiabilitas Pasal 4(1).	Tidak diatur secara eksplisit. Dapat tercakup secara implisit melalui pendekatan fungsional berdasarkan definisi luas Pasal 1 angka 1 sepanjang *inferred data* dapat mengidentifikasi individu.
Data sensitif/kategori khusus	Pasal 9(1): larangan mutlak pemrosesan data ras/etnis, agama, pandangan politik, serikat pekerja, genetik, biometrik, kesehatan, dan orientasi seksual. Pasal 9(2): sepuluh pengecualian. *Inferred data* dapat masuk kategori ini apabila inferensi mengungkap karakteristik sensitif.	Pasal 4 ayat (2): data spesifik mencakup data kesehatan, biometrik, genetika, kehidupan/orientasi seksual, pandangan politik, agama, keuangan, dan data anak. *Inferred data* yang mengungkap karakteristik ini dapat dikualifikasikan sebagai data spesifik.
B. *Profiling*dan Automated Decision-Making (ADM)		
Definisi profiling	Pasal 4(4): pemrosesan data pribadi secara otomatis untuk mengevaluasi aspek tertentu dari individu, termasuk kinerja, situasi ekonomi, kesehatan, preferensi, minat, perilaku, lokasi, atau pergerakan.	Tidak didefinisikan secara eksplisit. Dikonstruksi secara implisit melalui hak subjek data dalam Pasal 10 untuk menolak keputusan dari pemrosesan otomatis termasuk profiling.
Pengaturan ADM	Pasal 22(1): larangan umum keputusan semata-mata berbasis pemrosesan otomatis yang berdampak hukum signifikan. Pasal 22(2): tiga pengecualian (kontrak, kewajiban hukum, persetujuan eksplisit). Recital 71 memperjelas syarat dan safeguard.	Tidak ada pasal khusus ADM. Diatur secara implisit melalui Pasal 10 (hak keberatan terhadap keputusan otomatis) dan Pasal 34 (kewajiban PDPD/DPIA untuk pemrosesan berisiko tinggi). Ambang batas 'dampak signifikan' tidak didefinisikan.
Tiga bentuk profiling	Article 29 WP mengakui: (1) *profiling* umum tanpa keputusan; (2) keputusan berbasis profil dengan keterlibatan manusia; (3) keputusan sepenuhnya otomatis dengan dampak signifikan. Hanya bentuk ketiga yang tercakup Pasal 22.	UU PDP tidak membedakan secara eksplisit tiga bentuk *profiling* tersebut. Pengaturan cenderung bersifat umum dan tidak memilah tingkatan intervensi manusia dalam proses keputusan.
Peran *inferred data* dalam ADM	Diakui secara implisit melalui Recital 71: keputusan otomatis termasuk *profiling* harus disertai informasi yang memungkinkan individu memahami dasar penilaian. *Inferred data* sebagai output *profiling* menjadi input utama ADM.	Tidak diatur secara eksplisit. Hubungan *inferred data,* profiling ADM dapat dikonstruksi secara implisit melalui ketentuan hak keberatan dalam Pasal 10 dan kewajiban prinsip transparansi dalam Pasal 16 ayat (2).
C. Hak Subjek Data		
Hak atas informasi	Pasal 13 & 14: kewajiban pengendali memberikan informasi komprehensif termasuk tujuan pemrosesan, logika ADM, dan dampak signifikan. Recital 71 mensyaratkan penjelasan yang memungkinkan individu memahami dan menantang keputusan otomatis.	Pasal 5: hak mendapatkan informasi tentang identitas pengendali, dasar kepentingan hukum, tujuan permintaan, dan akuntabilitas. Cakupan informasi terkait logika ADM dan *inferred data* belum diatur secara eksplisit.

Hak akses	Pasal 15: hak akses terhadap data yang digunakan dalam pembentukan profil dan output inferensi, termasuk segmen atau kategori tempat individu ditempatkan.	Pasal 7: hak memperoleh akses dan salinan data pribadi. Namun belum ada ketentuan eksplisit yang menjawab apakah hak akses mencakup *inferred data* yang dihasilkan oleh pengendali.
Hak perbaikan data	Pasal 16: hak memperbaiki data tidak akurat termasuk data input maupun output inferensi. Pasal 18: hak pembatasan pemrosesan selama proses perbaikan berlangsung.	Pasal 6: hak pembaharuan, perbaikan, dan/atau penambahan data pribadi yang tidak akurat. Belum ada ketentuan eksplisit mengenai perbaikan *inferred data* yang dihasilkan melalui proses algoritmik.
Hak penghapusan	Pasal 17: hak penghapusan (right to erasure/right to be forgotten) dalam kondisi tertentu, termasuk jika data tidak lagi relevan dengan tujuan semula atau pemrosesan tidak memiliki dasar hukum yang sah.	Pasal 43-45: hak mengajukan permohonan penghapusan data yang sudah tidak relevan. Tidak bersifat mutlak dan harus mempertimbangkan kewajiban penyimpanan berdasarkan peraturan lain.
Hak keberatan terhadap ADM/profiling	Pasal 21: hak mengajukan keberatan terhadap profiling. Pasal 21(2): hak absolut keberatan terhadap *profiling* untuk pemasaran langsung. Pasal 22(3): hak meminta penilaian manusia, menyampaikan pendapat, dan menantang keputusan otomatis.	Pasal 10: hak menolak atau mengajukan keberatan terhadap keputusan semata-mata dari pemrosesan otomatis termasuk *profiling* yang menghasilkan dampak hukum atau mempengaruhi subjek data secara signifikan. Ambang batas 'signifikan' tidak didefinisikan.
Hak portabilitas data	Pasal 20: hak menerima data pribadi dalam format terstruktur dan dapat dibaca mesin, serta hak memindahkan data antar pengendali.	Pasal 9: hak mengirimkan atau menggunakan data pribadi ke pengendali data pribadi lainnya. Cakupan dan mekanisme teknis belum diatur secara rinci.
D. Transparansi dalam Pemrosesan *Inferred data* dan ADM		
Prinsip transparansi	Pasal 5(1)(a): lawfulness, fairness, and transparency sebagai prinsip dasar. Pasal 12-14: kewajiban pemberitahuan komprehensif. Recital 71: wajib memberikan penjelasan yang memungkinkan pemahaman dan penantangan keputusan otomatis.	Pasal 16 ayat (2): transparansi sebagai salah satu dari delapan prinsip dasar pemrosesan. Pengendali wajib memberitahukan tujuan dan aktivitas pemrosesan termasuk penggunaan data untuk menghasilkan *inferred data* .
Penjelasan logika ADM	Recital 71 & Pasal 22(3): pengendali wajib menyediakan informasi bermakna tentang logika yang digunakan, serta signifikansi dan konsekuensi yang diperkirakan dari pemrosesan terhadap subjek data.	Tidak diatur secara eksplisit. Kewajiban menjelaskan logika algoritma dan *inferred data* belum memiliki dasar normatif yang tegas dalam UU PDP.
DPIA/Penilaian dampak	Pasal 35: Data Protection Impact Assessment (DPIA) wajib dilakukan apabila pemrosesan berpotensi menghasilkan risiko tinggi, termasuk evaluasi sistematis individu berbasis *profiling* dan ADM berskala besar.	Pasal 34: Penilaian Dampak Perlindungan Data Pribadi (PDPD) wajib dilakukan apabila pemrosesan memiliki potensi risiko tinggi terhadap subjek data. Panduan teknis spesifik untuk ADM dan *profiling* belum tersedia.
Dokumentasi & akuntabilitas	Pasal 30: kewajiban menyimpan catatan kegiatan pemrosesan. Pasal 5(2): accountability principle mengharuskan pengendali mampu mendemonstrasikan kepatuhan.	Pasal 31: kewajiban perekaman seluruh kegiatan pemrosesan data pribadi. Pasal 47: prinsip akuntabilitas mewajibkan pengendali bertanggung jawab dan menunjukkan pertanggungjawaban.

Dasar hukum pemrosesan	Pasal 6(1): enam dasar hukum alternatif termasuk legitimate interests (Pasal 6(1)(f)) yang memberikan fleksibilitas bagi pengendali untuk memproses data untuk kepentingan bisnis yang sah.	Pasal 20 ayat (2): lima dasar hukum alternatif (persetujuan, perjanjian, kewajiban hukum, kepentingan vital, kepentingan umum). Tidak mengenal legitimate interests sehingga fleksibilitas pengendali lebih terbatas.
E. Kesenjangan dan Perbandingan Umum		
Tingkat eksplisitasi *inferred data*	Tidak didefinisikan secara eksplisit sebagai kategori mandiri, namun diakui melalui pedoman resmi (Article 29 WP) dan yurisprudensi yang berkembang.	Tidak diatur sama sekali secara eksplisit. Hanya dapat dikonstruksi secara implisit melalui interpretasi fungsional terhadap definisi data pribadi.
Kepastian hukum ADM	Relatif lebih tinggi: Pasal 22 secara eksplisit mengatur larangan, pengecualian, dan safeguard. Namun ambiguitas masih ada pada penerapan di konteks *profiling* multi-tahap.	Relatif lebih rendah: tidak ada pasal khusus ADM. Ketentuan tersebar implisit dalam berbagai pasal dan ambang batas 'dampak signifikan' tidak didefinisikan.
Otoritas pengawas	Supervisory Authority yang independen dan operasional di setiap negara anggota. Memiliki kewenangan investigasi, koreksi, dan sanksi yang kuat.	Lembaga Pelindungan Data Pribadi diamanatkan Pasal 58 namun belum terbentuk dan beroperasi secara penuh. Pengawasan masih bersifat sektoral.
Peraturan pelaksana	GDPR didukung oleh guidelines dari European Data Protection Board (EDPB) dan Article 29 WP yang komprehensif untuk berbagai aspek termasuk *profiling* dan ADM.	Peraturan pelaksana UU PDP (PP/Perpres) belum seluruhnya tersedia. Panduan teknis spesifik untuk pemrosesan otomatis, *profiling*, dan *inferred data* belum diterbitkan.

Tabel di atas menunjukkan bahwa meskipun keduanya menggunakan definisi data pribadi yang luas, GDPR jauh lebih eksplisit dalam mengatur *profiling* dan ADM beserta *safeguards* nya, sedangkan UU PDP mengandalkan pendekatan implisit yang bergantung pada interpretasi dan belum didukung oleh peraturan pelaksana yang memadai. Implikasinya adalah terdapat celah perlindungan yang signifikan dalam UU PDP, khususnya dalam aspek: (1) tidak adanya kewajiban penjelasan yang bermakna atas logika ADM kepada subjek data; (2) ketiadaan ambang batas "dampak signifikan" yang jelas sebagai pemicu hak keberatan; dan (3) tidak diakuinya legitimate interests sebagai dasar pemrosesan yang justru membatasi fleksibilitas sekaligus potensi penyalahgunaan.

5) Tantangan Implementasi dan Implikasi Praktis bagi Indonesia

Meskipun UU PDP telah memberikan kerangka hukum yang cukup komprehensif, efektivitas perlindungan terhadap risiko *inferred data* dalam praktik ADM masih menghadapi sejumlah tantangan serius. Pertama, terdapat kesenjangan antara aturan normatif dan kapasitas teknis implementasi, di mana banyak pengendali data, khususnya usaha mikro, kecil, dan menengah, masih memiliki pemahaman dan kapasitas terbatas dalam menerapkan ketentuan UU PDP. Kedua, kompleksitas teknologi ADM dan inferensi data membuat pengawasan dan penegakan hukum menjadi semakin menantang, terutama mengingat belum adanya panduan teknis spesifik mengenai pemrosesan otomatis, profiling, dan penggunaan *inferred data* yang menyebabkan ketidakpastian dalam implementasi praktis.

Berbagai penelitian mengenai efektivitas UU PDP menunjukkan bahwa meskipun substansi undang-undang tersebut sudah sejalan dengan prinsip-prinsip

perlindungan data global, pelaksanaannya di lapangan masih menghadapi kendala berupa kurangnya pemahaman masyarakat dan pelaku usaha, kesiapan teknologi dan infrastruktur yang belum optimal, belum terbentuknya otoritas pengawas independen, serta ketiadaan peraturan turunan teknis yang komprehensif (Sitorus et al., 2025). Secara kritis, kondisi ini menunjukkan bahwa perlindungan terhadap *inferred data* dalam UU PDP saat ini masih lebih bersifat normatif daripada efektif secara praktis, dan implikasinya adalah subjek data di Indonesia masih berada dalam posisi rentan terhadap risiko yang ditimbulkan oleh penggunaan *inferred data* dalam sistem ADM.

Dengan demikian, efektivitas perlindungan terhadap risiko *inferred data* dalam praktik ADM di Indonesia akan sangat bergantung pada: (1) terbentuknya peraturan pelaksana yang memberikan panduan teknis secara jelas dan rinci, khususnya mengenai *profiling* dan ADM; (2) pembentukan serta operasionalisasi Lembaga Pelindungan Data Pribadi sebagai otoritas pengawas independen yang diamanatkan Pasal 58 UU PDP; (3) peningkatan kesadaran dan kapasitas baik di kalangan pengendali data maupun subjek data; serta (4) pengembangan praktik terbaik dalam industri yang sejalan dengan prinsip-prinsip perlindungan data pribadi, dengan mengacu pada pengalaman implementasi GDPR sebagai tolok ukur komparatif.

KESIMPULAN

Baik GDPR maupun UU PDP memberikan kerangka perlindungan terhadap risiko *inferred data* dalam sistem *automated decision-making* (ADM), namun dengan pendekatan yang berbeda. GDPR mengatur secara eksplisit melalui Pasal 22 dengan larangan keputusan otomatis berdampak signifikan dan hak atas penjelasan algoritmik, sementara UU PDP hanya memberikan perlindungan secara implisit melalui pendekatan fungsional yang belum setara. Kesenjangan ini menjadi kelemahan struktural yang mendesak untuk diatasi, mengingat praktik ADM berbasis inferensi algoritmik terus berkembang pesat di Indonesia. Oleh karena itu, pemerintah selaku pembuat kebijakan perlu segera menerbitkan peraturan pelaksana UU PDP yang mengklasifikasikan *inferred data* secara eksplisit sebagai data berisiko tinggi, sekaligus mengadopsi prinsip *right to explanation* sebagaimana Recital 71 GDPR sebagai hak yang dapat dituntut secara hukum, sehingga subjek data memiliki instrumen konkret untuk mempersoalkan keputusan otomatis yang merugikan mereka.

REFERENSI

Abrams, M. (2014). The Origins of Personal Data and its Implications for Governance. *Social Science Research Network*, 1–12. https://doi.org/10.2139/ssrn.2510927

Agustina, W., & Wiraguna, S. A. (2025). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten : Riset Hukum dan Hak Asasi Manusia*, *2*(6), 117–127. https://doi.org/10.52005/rechten.v4i2.98

Andini, K. (2026). Implikasi Yuridis Undang-Undang Perlindungan Data Pribadi terhadap Model Bisnis Digital di Indonesia. *Journal of Innovative and Creativity*, *6*(1), 9400–9414.

Attamongkol, T., & Putra, E. N. (2025). Data Protection in Thailand and Indonesia: Struggling and Striving for European-Like Privacy. *Social Science Research Network*, 1–33. https://doi.org/http://dx.doi.org/10.2139/ssrn.5341565

Barn, B. S. (2020). Mapping The Public Debate On Ethical Concerns: Algorithms In Mainstream Media. *Journal of Information, Communication and Ethics in Society*, *18*(1), 124–139. https://doi.org/https://doi.org/10.1108/JICES-04-2019-0039

Choroszewicz, M. (2026). Positioning public sector practitioners as 'moral crumple zones': Mechanisms in the early use of generative AI work support tools. *Government Information Quarterly*, *42*(2), 1–15.

https://doi.org/https://doi.org/10.1016/j.giq.2026.102128
Custers, B., & Vrabec, H. (2024). Tell Me Something New Data Subject Rights Applied to *Inferred data* and Profiles. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, *52*, 1–14. https://doi.org/10.1016/j.clsr.2024.105956
Dham, V., Rai, K., & Soni, U. (2021). Mental Stress Detection Using Artificial Intelligence Models. *Journal of Physics: Conference Series*, *1950*, 1–10. https://doi.org/10.1088/1742-6596/1950/1/012047
Guidelines on the Right to Data Portability. (2017). https://ec.europa.eu/newsroom/dae/redirection/document/44099
Häuselmann, A., & Custers, B. (2024). The Right to Rectification and Inferred Personal Data. *European Journal of Law and Technology*, *15*(3).
Holtz, H. M., & Ledendal, J. (2026). AI Data Governance-Overlaps between the AI Act and the GDPR. *Law, Innovation and Technology*, *18*(6), 1–30. https://doi.org/https://doi.org/10.1080/17579961.2026.2633677
Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private Traits and Attributes are Predictable From Digital Records of Human Behavior. *Proc. Natl. Acad. Sci. U.S.A*, *110*(15), 2–5. https://doi.org/10.1073/pnas.1218772110
Li, L., Wang, J., Wang, X., Peng, P., Shen, J., Zhu, H., & Zhang, Z. (2025). Big Data And Data Science In Global Governance: Anticipating Future Needs And Applications In The UN And Beyond. *Front. Polit*, *7*, 1–25. https://doi.org/10.3389/fpos.2025.1583772
Matsumi, H., & Solove, D. J. (2024). The Prediction Society: AI and The Problems of Forecasting The Future. *GWU Legal Studies Research Paper*, *1*, 1–62. https://doi.org/http://dx.doi.org/10.2139/ssrn.4453869
Parluhutan, D. (2021). Analisis Hukum Kompetisi terhadap "Big Data" dan Doktrin "Essential Facility" dalam Transaksi Mergerdi Indonesia. *Jurnal Persaingan Usaha*, *1*(1), 84–97.
Party, A. 29 D. P. W. (2018). *Guidelines on Automated Individual Decision-Making and Profilingfor the Purposes of Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/612053
Pradana, M. A. E., & Saragih, H. (2024). Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR dan Akibat Hukumnya. *Innovative Journal of Social Science Research*, *4*(4), 3412–3425.
Sitorus, R., Saragih, J. Z. F., & Banke, R. (2025). Kendala Pelaksanaan Perlindungan Data Pribadi. *Locus: Jurnal Konsep Ilmu Hukum*, *5*(1), 54–61. https://doi.org/10.56128/jkih.v4i3.402
Tamim, J. (2024). The Brussels Effect and the GDPR: EU Institutions as Catalysts for Global Data Protection Norms. In *European Digital Policy Initiative (EDPI)*. https://doi.org/10.13140/RG.2.2.28132.59529
Wachter, S., & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, *2*, 1–85. https://doi.org/10.31228/osf.io/mu2kf
Wahyuningtyas, S. Y. (2024). Implikasi Algorithmic Decision-Making (ADM) Terhadap Otonomi Subyek Data dan Legalitasnya Dalam Pemrosesan Big Data. *Jurnal Paradigma Hukum Pembangunan*, *9*(2), 150–189. https://doi.org/10.25170/paradigma.v9i2.5890
Wiedemann, K. (2022). *Profiling*and (Automated) Decision Making Under the GDPR: A Two-Step Approach. *Computer Law & Security Review*, *45*(1), 1–17. https://doi.org/https://doi.org/10.1016/j.clsr.2022.105662