E-NISN : 2614-2643
P-NISN : 2541-7037
Journal Equitable
Vol 10 No 3
2025

PERBANDINGAN REGULASI PERLINDUNGAN DATA PRIBADI ANTARA INDONESIA DAN SINGAPURA DALAM KONTEKS KASUS *WORLDCOIN*

Mohamad Gery Alfaaiz
Universitas Pelita Harapan, Indonesia, 01659240010@student.uph.edu

Abstract

This study examines the comparative regulation of personal data protection between Indonesia and Singapore in the context of the Worldcoin case, a global project collecting biometric data through iris scanning. The central research question concerns the differences in legal frameworks for protecting biometric data and their implications for citizen protection. This research adopts a normative legal method with a comparative and case study approach. The findings reveal that Indonesia's Law No. 27 of 2022 on Personal Data Protection explicitly classifies biometric data as specific personal data requiring explicit consent. However, Indonesia lacks a dedicated supervisory authority and has limited technical regulation concerning specific biometric types such as iris scans. On the other hand, Singapore's Personal Data Protection Act (PDPA) provides a principle-based framework that offers flexibility regarding consent and accountability, supported by an active supervisory body (PDPC). These differing approaches influence how each country responds to the Worldcoin initiative: Singapore opted for regulatory audits, while Indonesia suspended activities based on administrative discretion. The study recommends strengthening institutional oversight and enhancing Indonesia's technical regulation to address biometric technologies more effectively and adaptively.

Keywords: *Biometrics, Data Protection, Indonesia, Iris, Singapore*

Abstrak

Studi ini membahas perbandingan regulasi perlindungan data pribadi antara Indonesia dan Singapura dalam konteks kasus Worldcoin, sebuah proyek global yang mengumpulkan data biometrik berupa pemindaian iris. Rumusan masalah dalam penelitian ini adalah bagaimana perbandingan kerangka hukum kedua negara dalam melindungi data biometrik, serta implikasinya terhadap perlindungan warga negara. Metode yang digunakan adalah yuridis normatif dengan pendekatan perbandingan hukum dan studi kasus. Hasil penelitian menunjukkan bahwa Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi di Indonesia memiliki ketentuan eksplisit mengenai data biometrik sebagai data pribadi spesifik yang memerlukan persetujuan eksplisit. Namun, Indonesia belum memiliki lembaga otoritas pengawas khusus, serta belum mengatur secara teknis perlindungan untuk semua jenis biometrik seperti iris. Sementara itu, Personal Data Protection Act (PDPA) di Singapura memberikan kerangka hukum berbasis prinsip dengan fleksibilitas dalam hal persetujuan dan tanggung jawab pengendali data, serta dilengkapi otoritas pengawas yang aktif (PDPC). Perbedaan pendekatan ini berpengaruh langsung terhadap respons negara terhadap proyek Worldcoin, di mana Singapura memilih jalur audit dan pengawasan, sedangkan Indonesia menempuh penghentian kegiatan secara administratif. Studi ini menyarankan penguatan kelembagaan dan penyempurnaan teknis dalam regulasi Indonesia agar mampu menanggapi isu teknologi biometrik secara lebih adaptif.

Kata kunci: Biometrik, Indonesia, Iris, Perlindungan Data Pribadi, Singapura

A. Pendahuluan

Perkembangan teknologi informasi telah memudahkan berbagai lapisan masyarakat dalam beraktivitas sehari-hari, baik dalam dunia pendidikan maupun ekonomi, dengan meningkatkan kecepatan dan efisiensi pengumpulan informasi. Kemajuan teknologi juga mengubah kebutuhan masyarakat terhadap alat pembayaran, menuntut kecepatan, ketepatan, dan keamanan dalam transaksi elektronik, di mana alat pembayaran telah berevolusi dari bentuk fisik seperti logam dan uang kertas menjadi digital, seperti pembayaran elektronik.[1] Selain itu, teknologi membuka peluang bisnis untuk berkembang dan bersaing di era kompetitif, di mana perusahaan dapat memanfaatkan platform digital seperti *e-commerce* dan media sosial untuk menjangkau pasar lebih luas, meningkatkan pendapatan, serta mengoptimalkan biaya melalui pengelolaan data yang efektif.[2]

Di era digital saat ini, data telah menjadi faktor produksi penting dalam industri. Data dikumpulkan, diolah, dikelola, dan didistribusikan untuk memberikan *insight* bisnis yang berguna, seperti memahami perilaku konsumen, tren pasar, dan kinerja operasional perusahaan. Dengan memanfaatkan data terutama data pribadi pelanggan perusahaan dapat mengidentifikasi peluang bisnis dan mengambil keputusan yang lebih tepat. Namun, penggunaan data pribadi harus didasarkan pada prinsip keamanan, kehati-hatian, dan kerahasiaan. Salah satu jenis data yang dinilai relatif aman dari ancaman pembobolan atau penyalahgunaan adalah

[1] Amar Ahmad, Perkembangan Teknologi Komunikasi dan Informasi, Universitas Brawijaya, Jakarta, 2012, hlm. 138

[2] Rian Mangapul Sirait, Tantangan Hukum Penggunaan Data Biometrik dalam Keperluan Bisnis, *Jurnal Konseling Pendidikan Islam*, Vol.4. No.2 Juli 2023.

data biometrik, seperti retina mata, meskipun tidak sepenuhnya bebas dari risiko.[3]

Dalam pengolahan data pribadi, terutama yang bersifat spesifik seperti data biometrik, teknologi pendukung seperti *Artificial Intelligence* (AI) kini memainkan peran penting. AI adalah ilmu dan rekayasa untuk membuat mesin cerdas, terutama program komputer yang mampu melakukan tugas-tugas yang biasanya membutuhkan kecerdasan manusia.[4] AI memungkinkan pemrosesan data dalam jumlah besar secara otomatis, cepat, dan akurat, termasuk dalam hal identifikasi dan autentikasi individu. Namun, keunggulan ini juga membawa tantangan baru terhadap perlindungan privasi. Perkembangan sistem biometrik retina yang dikombinasikan dengan *Artificial Intelligence* (AI) menawarkan tingkat akurasi identifikasi yang sangat tinggi. Pola pembuluh darah retina yang unik dan stabil menjadikannya salah satu metode autentikasi paling aman dibandingkan jenis biometrik lainnya.[5]

Integrasi dengan AI memungkinkan sistem terus belajar dan meningkatkan akurasinya secara mandiri seiring waktu. Namun, penggunaan teknologi ini menghadapi tantangan serius dalam hal perlindungan privasi. Kemampuan AI untuk mengumpulkan dan memproses data biometrik secara otomatis berpotensi melanggar prinsip persetujuan pengguna. Yang lebih mengkhawatirkan, sifat permanen data retina membuat risiko kebocoran data menjadi masalah kritis, karena tidak seperti password, data

[3] Mauro Barni, Iris Deidentification With High Visual Realism for Privacy Protection on Websites and Social Networks, *IEEE Access,* Vol 9, 2021, hlm. 131996

[4] Stuart Russell dan Peter Norvig, *Artificial Intelligence: A Modern Approach, 4th ed*, Pearson, New York, 2021, hlm. 1

[5] Fahreddin Sadikoglu, Biometric Retina Identification Based On Neural Network, *Procedia Computer Science*, Volume 102, 2016, hlm. 27

biometrik tidak dapat diubah jika sudah terekspos. Isu etis seperti pengumpulan data berlebihan (*data spillover*) dan penggunaan di luar tujuan awal (*data repurposing*) semakin mengemuka seiring meluasnya penerapan teknologi ini. Tantangan ini memerlukan kerangka regulasi yang kuat untuk menyeimbangkan inovasi teknologi dengan perlindungan hak privasi individu.[6]

Sebagai contoh nyata, praktik pengumpulan data biometrik tanpa persetujuan dapat dilihat pada kasus *Clearview AI Inc.* Perusahaan yang berbasis di Amerika Serikat ini membangun database biometrik dengan mengumpulkan foto wajah dari berbagai sumber publik di internet, kemudian mengubahnya menjadi data biometrik berupa *face print*. Yang menjadi masalah, *Clearview* melakukan pengumpulan data tersebut tanpa memberitahu maupun meminta persetujuan dari pemilik data, sebagaimana diungkapkan dalam investigasi oleh *Information Commissioner's Office* (ICO) tahun 2022. Praktik ini jelas melanggar berbagai ketentuan perlindungan data pribadi yang berlaku di banyak negara.[7]

Selain kasus *Clearview AI*, kekhawatiran terhadap perlindungan data pribadi biometrik terjadi dalam kasus *Worldcoin*, sebuah proyek global yang yang didirikan oleh Sam Altman, CEO *OpenAI*, melalui entitas bernama *Tools for Humanity* dengan misi untuk membangun sistem identitas digital berbasis verifikasi biometrik melalui pemindaian iris mata. Untuk mendukung sistem tersebut, *Worldcoin* menyebarkan perangkat pemindai biometrik

[6] Gaurav Malik, *Biometric Authentication-Risks And Advancements In Biometric Security Systems*, Journal of Computer Science and Technology Studies, Vol 6 No 3, hlm. 165

[7] Jack Thorne, *Clearview AI Inc v the ICO: Where Technology and Data Protection Collide*, 2023, https://www.mwe.com/insights/clearview-ai-inc-v-the-ico-where-technology-and-data-protection-collide/

yang disebut "*Orb"* ke berbagai negara, termasuk Indonesia dan Singapura. Di Indonesia, *Worldcoin* melakukan pemindaian iris terhadap masyarakat tanpa transparansi yang memadai mengenai pengumpulan, penyimpanan, dan penggunaan data biometrik yang diperoleh. Sementara itu, di Singapura, otoritas setempat bergerak cepat dan tegas; pada Januari 2024, *Personal Data Protection Commission* (PDPC) menyatakan bahwa pihaknya sedang melakukan investigasi terhadap kegiatan *Worldcoin* karena diduga melanggar ketentuan dalam *Personal Data Protection Act (PDPA)* Singapura, termasuk prinsip-prinsip persetujuan eksplisit, pemrosesan yang wajar, dan pembatasan tujuan.[8]

[8] Cahyandaru Kuncorojati, *Diprotes Banyak Negara, Apakah World App Aman?*, 2025, https://www.medcom.id/teknologi/news-teknologi/JKR5eZVk-diprotes-banyak-negara-apakah-world-app-aman

Gambar 1
Logo Worldcoin

Ketegasan PDPC Singapura menjadi cerminan bagaimana sistem regulasi dan penegakan hukum perlindungan data pribadi yang terstruktur mampu merespons ancaman terhadap privasi dengan cepat. Hal ini kontras dengan kondisi di Indonesia, yang meskipun telah memiliki regulasi yakni Undang-Undang Nomr 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP), namun masih menghadapi tantangan dalam hal implementasi dan kelembagaan, termasuk belum efektifnya pembentukan otoritas perlindungan data yang independen seperti di Singapura. Kasus *Worldcoin* menjadi ilustrasi nyata bagaimana perbedaan regulasi dan kelembagaan antara dua negara

dapat berdampak langsung pada perlindungan hak data pribadi warga negaranya.

Regulasi mengenai perlindungan data pribadi di Indonesia dan Singapura menunjukkan perbedaan mendasar, baik dari aspek norma hukum maupun kelembagaan. Di Indonesia, regulasi utama adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang mengatur prinsip-prinsip pemrosesan data pribadi, hak-hak subjek data, serta kewajiban pengendali dan prosesor data. UU PDP mengkategorikan data biometrik sebagai data pribadi yang bersifat spesifik, sehingga tunduk pada persyaratan ketat dalam hal pemrosesan, termasuk persetujuan eksplisit dari subjek data. Namun, hingga saat ini, pelaksanaan UU PDP masih menghadapi hambatan, terutama karena belum terbentuknya otoritas independen sebagai pengawas pelaksanaan undang-undang ini. Sebaliknya, di Singapura, *Personal Data Protection Act (PDPA)* telah berlaku sejak tahun 2012 dan telah mengalami beberapa revisi yang memperkuat perlindungan bagi subjek data. PDPA mewajibkan adanya persetujuan eksplisit sebelum data dikumpulkan, serta menerapkan prinsip-prinsip seperti *notification obligation, purpose limitation*, dan *accountability*. PDPC sebagai lembaga pengawas yang telah mapan memiliki kewenangan investigasi, penegakan hukum, hingga pemberian sanksi administratif, sehingga implementasi PDPA lebih terjamin dan efisien. Perbandingan ini menunjukkan bahwa keberadaan lembaga pengawas yang kuat dan independen merupakan faktor kunci keberhasilan dalam perlindungan data pribadi, terutama dalam menghadapi tantangan baru seperti penggunaan data biometrik oleh entitas global seperti *Worldcoin.*

Meski regulasi perlindungan data pribadi telah ada, Indonesia masih menghadapi tantangan serius dalam hal kebocoran data. Berdasarkan catatan Kominfo, terjadi 98 kasus kebocoran data dari 2016 hingga 2024, dengan beberapa insiden besar yang melibatkan jutaan data sensitif.[9] Pada tahun 2022, misalnya, peretas Bjorka berhasil membobol data BPJS Ketenagakerjaan, mengekspos 19,5 juta data berisi NIK, nama lengkap, tanggal lahir, dan informasi pribadi lainnya. Tidak hanya itu, pada Mei 2023, 34,9 juta data paspor WNI bocor dan bahkan diperdagangkan secara ilegal, mencakup detail seperti nama, tanggal berlaku paspor, dan informasi kependudukan lengkap.[10] Kebocoran data semakin parah dengan lemahnya pengawasan. Salah satu contohnya adalah kasus Bank Syariah Indonesia (BSI) yang mengalami pembobolan 1,5 TB data oleh kelompok peretas *LockBit*, termasuk 15 juta kredensial pengguna dan data nasabah.[11] Masalah ini diperburuk oleh praktik jual-beli data pribadi oleh oknum perusahaan, seperti yang terjadi pada beberapa bank yang menjual data nasabah kartu kredit tanpa izin. Tanpa pengawasan yang ketat dan penegakan hukum yang konsisten, kerentanan kebocoran data akan terus menjadi ancaman serius bagi privasi masyarakat.

[9] Komdigi, *Siaran Pers No. 138/HM/KOMINFO/07/2023 tentang Perkembangan Penanganan Dugaan Kebocoran Data Paspor 34,9 Juta Warga Indonesia*, 2023, https://www.komdigi.go.id/berita/siaran-pers/detail/siaran-pers-no-138-hm-kominfo-07-2023-tentang-perkembangan-penanganan-dugaan-kebocoran-data-paspor-34-9-juta-warga-indonesia

[10] Maria Fransisca Lahur, *Datanya Diduga Dibobol Bjorka*, BPJS Malah Dipuji Pakar, 2023, https://www.tempo.co/digital/datanya-diduga-dibobol-bjorka-bpjs-malah-dipuji-pakar-208711

[11] CNNIndonesia, *Lockbit 3.0 Diduga Curi Data dan Password 15 Juta Nasabah BSI*, 2023, https://www.cnnindonesia.com/ekonomi/20230513102703-92-949058/lockbit-30-diduga-curi-data-dan-password-15-juta-nasabah-bsi

Di Indonesia, penggunaan teknologi biometrik dalam konteks identifikasi telah memiliki dasar hukum, salah satunya melalui Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 37 Tahun 2016 tentang Tata Cara Pengambilan, Perumusan, dan Identifikasi Teraan Sidik Jari. Peraturan ini mengatur secara teknis proses pengambilan, penyimpanan, dan penggunaan data sidik jari sebagai sarana identifikasi dalam kepentingan hukum, khususnya dalam proses perumusan identitas seseorang yang terkait dengan tindak pidana atau kebutuhan forensik. Peraturan ini mencerminkan langkah awal pemerintah dalam melegitimasi penggunaan data biometrik sebagai alat identifikasi. Namun demikian, cakupannya masih terbatas karena belum menyentuh aspek pemrosesan data pribadi secara lebih luas, termasuk perlindungan terhadap data biometrik oleh pihak swasta, keamanan pemrosesan data, dan tanggung jawab pengendali data.

Permasalahan yuridis dalam penerapan teknologi biometrik muncul ketika data yang dikumpulkan tidak hanya digunakan oleh instansi negara, tetapi juga dimanfaatkan oleh entitas non-pemerintah. Hal ini menimbulkan kekhawatiran akan potensi pelanggaran terhadap hak privasi dan perlindungan data pribadi, terutama apabila pemrosesan data dilakukan tanpa persetujuan eksplisit dari subjek data. Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), data biometrik tergolong sebagai data pribadi spesifik yang memerlukan perlindungan ekstra. Pasal 20 ayat (2) UU PDP menegaskan bahwa pemrosesan data pribadi spesifik hanya dapat dilakukan dengan persetujuan eksplisit dari pemilik data. Hal ini menegaskan bahwa setiap bentuk penggunaan teknologi

biometrik, baik oleh negara maupun swasta, harus tunduk pada prinsip legitimasi hukum, transparansi, dan akuntabilitas.

Kebutuhan akan tinjauan ulang dan harmonisasi regulasi menjadi sangat mendesak mengingat perkembangan teknologi biometrik yang semakin kompleks dan lintas batas. Indonesia masih menghadapi tantangan dalam mengatur penggunaan data biometrik di luar konteks keperluan forensik, misalnya untuk layanan keuangan, asuransi, maupun proyek berbasis kripto seperti *Worldcoin*. Ketiadaan regulasi turunan UU PDP yang spesifik mengatur biometrik, serta lemahnya kapasitas kelembagaan seperti Otoritas Perlindungan Data Pribadi (yang belum sepenuhnya terbentuk), menjadikan implementasi perlindungan data belum optimal. Dibandingkan dengan Singapura, yang telah menerapkan *Personal Data Protection Act (PDPA)* secara komprehensif sejak 2012 dan memiliki lembaga otoritatif seperti *Personal Data Protection Commission* (PDPC), Indonesia masih tertinggal dalam aspek kelembagaan dan penegakan hukum terhadap pelanggaran data biometrik. Oleh karena itu, diperlukan perumusan kebijakan yang lebih spesifik dan komprehensif guna menjawab tantangan teknologi biometrik dalam konteks perlindungan hak asasi digital masyarakat.

Meskipun Indonesia telah memiliki regulasi seperti Peraturan Menteri Hukum dan HAM Nomor 37 Tahun 2016 dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dalam praktiknya masih terdapat berbagai tantangan implementatif terutama terkait perlindungan data biometrik seperti retina. Hal ini menjadi penting mengingat potensi penyalahgunaan data semakin meningkat seiring masifnya penggunaan teknologi biometrik oleh korporasi internasional,

seperti yang tampak dalam kasus *Worldcoin*. Sementara itu, Singapura telah lebih dahulu memiliki *Personal Data Protection Act* (PDPA) dan otoritas perlindungan data khusus yaitu *Personal Data Protection Commission* (PDPC), yang dapat menjadi tolok ukur bagi Indonesia dalam membangun sistem perlindungan data pribadi yang lebih responsif terhadap ancaman teknologi lintas batas. Perbandingan kedua negara dalam menangani perlindungan data pribadi, khususnya data biometrik dalam konteks kasus *Worldcoin*, menjadi relevan untuk dikaji secara mendalam. Oleh karena itu, penulis mengangkat judul "Perbandingan Regulasi Perlindungan Data Pribadi antara Indonesia dan Singapura dalam Konteks Kasus *Worldcoin*" sebagai bentuk kontribusi dalam memahami kesiapan regulasi nasional dalam menghadapi tantangan global terhadap keamanan data pribadi.

B. Rumusan Masalah

Dengan Latar Belakang penelitian tersebut maka dapat di rumuskan sebagai berikut:

Bagaimana Perbandingan Regulasi Perlindungan Data Pribadi antara Indonesia dan Singapura dalam Konteks Kasus *Worldcoin?*

C. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah untuk mengetahui bagaimana perbandingan regulasi perlindungan data pribadi antara Indonesia dan Singapura dalam konteks kasus *Worldcoin*.

D. Metode Penelitian

Jenis penelitian hukum yang digunakan adalah penelitian hukum normatif, yaitu penelitian yang memiliki objek kajian tentang kaidah atau aturan hukum. Penelitian hukum normatif meneliti kaidah atau peraturan hukum sebagai suatu

bangunan sistem yang terkait dengan suatu peristiwa hukum.[12] Sehingga di sini penulis akan meneliti data-data sekunder yang peneliti peroleh yang berhubungan dengan masalah yang peneliti angkat. Untuk sifatnya adalah deskriptif analitis.[13] Analisis data dalam penelitian kualitatif, dilakukan pada saat pengumpulan data berlangsung, dan setelah selesai pengumpulan data dalam periode tertentu.[14]

E. Hasil Penelitian dan Pembahasan

Perbandingan Regulasi Perlindungan Data Pribadi antara Indonesia dan Singapura dalam Konteks Kasus *Worldcoin*

1. Perbandingan Regulasi Perlindungan Data Pribadi antara Indonesia dan Singapura

Dalam membandingkan regulasi perlindungan data pribadi antara Indonesia dan Singapura, penting untuk terlebih dahulu menyoroti posisi hukum terkait data biometrik, terutama dalam konteks pemindaian iris sebagaimana digunakan oleh proyek *Worldcoin*. Data biometrik merupakan kategori data pribadi yang paling sensitif karena melekat pada karakteristik fisik yang unik dan permanen dari individu. Baik UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) maupun *Personal Data Protection Act* 2012 (PDPA) Singapura sama-sama mengakui sensitivitas ini, namun dengan pendekatan yang berbeda.

Di Indonesia, Pasal 4 ayat (1) huruf a UU PDP secara eksplisit mengkategorikan data biometrik sebagai bagian dari data pribadi spesifik, yang hanya boleh diolah berdasarkan persetujuan eksplisit tertulis dari subjek data (Pasal 20 ayat 1).

[12] Mukti Fajar dan Yulianto Achmad, *Dualisme Penelitian Hukum Normatif dan Empiris*, Cetakan IV, Pustaka Pelajar, Yogyakarta, 2017, hlm. 36

[13] Satjipto Rahardjo, *Sosiologi Hukum Perkembangan Metode dan Pilihan Masalah*, (Surakarta: Penerbit Muhammadiyah, 2004), hlm 1.

[14] Sugiyono, *Memahami Penelitian Kualitatif*, Alfabeta, Bandung, 2012, hlm. 91.

Penekanan pada bentuk persetujuan eksplisit ini menunjukkan pendekatan yang ketat terhadap perlindungan privasi, di mana pemrosesan tanpa dasar hukum yang sah dianggap sebagai pelanggaran serius. Lebih lanjut, dalam konteks teknis, Permenkumham No. 37 Tahun 2016 mengatur tentang tata cara pengumpulan dan penyimpanan data sidik jari untuk sistem administrasi hukum, termasuk penggunaan teknologi enkripsi dan standar penyimpanan khusus (Pasal 28).

Sementara itu, di Singapura, PDPA tidak menyebut secara spesifik jenis data biometrik seperti iris atau retina, namun dokumen resmi yang diterbitkan oleh Personal Data Protection Commission (PDPC), yaitu "*Guide on Responsible Use of Biometric Data in Security Applications*",[15] menjelaskan bahwa data biometrik mencakup sampel iris, sidik jari, dan wajah (Part I, hlm. 6). Ini menunjukkan bahwa pemindaian iris secara substantif diakui sebagai data pribadi sensitif di bawah kerangka hukum PDPA, meskipun tidak secara eksplisit tercantum dalam undang-undang.

Indonesia menerapkan sistem yang mewajibkan persetujuan eksplisit secara tertulis, tanpa adanya fleksibilitas yang signifikan, kecuali dalam hal-hal tertentu seperti penegakan hukum atau keselamatan publik (Pasal 20 ayat 2 UU PDP). Sebaliknya, Singapura menerapkan pendekatan yang lebih fleksibel berbasis risiko. Menurut Part III dokumen panduan PDPC (hlm. 15–19), persetujuan dapat dikecualikan dalam beberapa kondisi, seperti penggunaan untuk tujuan keamanan,

[15] Personal Data Protection Commission Singapore, *Guide on Responsible Use of Biometric Data in Security Applications*, 2023, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Guide-on-Responsible-Use-of-Biometric-Data-in-Security-Applications.pdf.

kepentingan sah organisasi, atau ketika data dikumpulkan di area publik. Pendekatan ini memberikan ruang bagi organisasi seperti *Worldcoin* untuk memproses data biometrik iris jika mereka dapat menunjukkan manfaat yang seimbang dengan risiko.

UU PDP Indonesia mewajibkan pengendali data untuk menjaga keamanan data pribadi dan menghapus data yang tidak relevan (Pasal 39 dan Pasal 16 huruf c). Permenkumham No. 37 Tahun 2016 memperkuat ini dengan mewajibkan penggunaan algoritma enkripsi dan pemisahan database antara data biometrik dan identitas (Pasal 28). Di sisi lain, dokumen PDPC Singapura menekankan minimalisasi data, hanya menyimpan template biometrik dan bukan sampel mentah, serta penghapusan data jika tidak lagi diperlukan (Part II, hlm. 11–13).

Singapura juga mengatur akuntabilitas organisasi atas data yang diproses oleh pihak ketiga (*vendor atau data intermediary*) sebagaimana diatur dalam *Part* III hlm. 22 dari panduan PDPC. Hal ini mirip dengan Pasal 56 UU PDP Indonesia, yang mewajibkan adanya perlindungan data yang setara di negara tujuan jika data dikirim ke luar negeri, serta kontrak yang mengikat dengan pihak penerima data.

Dalam hal sanksi, UU PDP Indonesia menetapkan ancaman pidana berupa penjara maksimal 6 tahun dan denda hingga Rp6 miliar untuk pelanggaran berat seperti pengumpulan tanpa persetujuan atau penyalahgunaan data pribadi (Pasal 67–68). Sementara itu, PDPA Singapura pada awalnya hanya mengenakan denda administratif maksimal SGD 1 juta, sebagaimana dimungkinkan melalui *Section* 29(2)(d). Namun, berdasarkan amandemen PDPA yang berlaku mulai 1 Oktober 2022, *Section* 48J memperluas ketentuan sanksi: organisasi dapat dikenakan denda hingga

10% dari omset tahunan mereka di Singapura jika pendapatannya melebihi SGD 10 juta.

Sebagai catatan penting, teknologi yang digunakan *Worldcoin* adalah pemindaian iris, bukan retina. Keduanya memang termasuk dalam kategori biometrik mata, namun memiliki perbedaan teknis. Pemindaian iris merekam pola warna pada bagian depan mata (iris), yang lebih mudah dipindai dan tidak terlalu invasif. Sementara itu, pemindaian retina memerlukan cahaya inframerah untuk menangkap pola pembuluh darah di bagian belakang mata. [16] Karena itu, penggunaan istilah "retina" dalam beberapa pemberitaan di Indonesia sebenarnya kurang tepat. Dokumen resmi dari PDPC Singapura pun hanya menyebut iris, bukan retina, sebagai cakupan data biometrik. Oleh karena itu, dalam penelitian ini, fokus analisis diarahkan pada pemindaian iris sebagai praktik aktual *Worldcoin*.

Perbandingan ini menunjukkan bahwa Indonesia memiliki kelebihan dalam bentuk pengakuan eksplisit terhadap data biometrik sebagai kategori data pribadi spesifik dan keharusan persetujuan eksplisit tertulis. Namun, kelemahan terletak pada belum adanya pengaturan teknis spesifik untuk biometrik iris, karena regulasi yang ada masih berfokus pada sidik jari. Singapura, meskipun tidak menjabarkan jenis biometrik secara eksplisit dalam PDPA, memberikan kerangka hukum yang lebih adaptif dan berbasis prinsip, yang memungkinkan perlindungan tetap relevan seiring berkembangnya teknologi seperti pemindaian iris oleh *Worldcoin*. Perbedaan pendekatan ini menjadi dasar penting dalam menilai efektivitas regulasi masing-masing negara dalam konteks praktik global saat ini.

[16] Sugandha Agarwal, A Comparative Study of Facial, Retinal, Iris and Sclera Recognition Techniques, *IOSR Journal of Computer Engineering*, Volume 16 Issue 1, 2014, hlm. 48

Tabel berikut menyajikan perbandingan aspek-aspek utama dalam regulasi perlindungan data biometrik, khususnya data iris atau scan biometrik yang relevan dengan kasus *Worldcoin*, antara Indonesia dan Singapura:

Tabel 3.1
Perbandingan Regulasi Perlindungan Data Biometrik Indonesia dan Singapura

Aspek	Indonesia (UU PDP No. 27/2022 & Permenkumham 37/2016)	Singapura (PDPA dan Regulasi terkait)
Klasifikasi Data Biometrik	Data biometrik termasuk dalam data pribadi spesifik yang memerlukan perlindungan khusus (UU PDP Pasal 4)	Data biometrik termasuk data sensitif yang harus dijaga kerahasiaannya (PDPA *Section* 2)
Persetujuan Penggunaan	Persetujuan eksplisit wajib diberikan untuk pengumpulan dan penggunaan data biometrik (UU PDP Pasal 20)	Persetujuan fleksibel dengan pengecualian untuk kepentingan sah seperti keamanan publik (PDPA *Sections* 13-16 dan *Guide Part* III)
Jenis Data Biometrik yang Diatur	UU PDP mengatur secara umum perlindungan data biometrik, sedangkan teknis pengaturan jenis data biometrik, seperti sidik jari, diatur oleh Permenkumham No. 37/2016 (Pasal 28)	Mencakup sampel dan template biometrik termasuk iris (*Guide Part* I dan III)
Keamanan dan Penyimpanan Data	Standar teknis ketat untuk penyimpanan data sidik jari, termasuk enkripsi dan penghapusan data (Permenkumham Pasal 28)	Enkripsi wajib, minimalisasi data, segregasi database, dan penghapusan data tidak perlu (*Guide Part* II)
Transfer Data ke Luar Negeri	Diatur ketat, hanya diizinkan ke negara dengan perlindungan setara (UU PDP Pasal 56)	Diizinkan dengan akuntabilitas pengendali data dan kontrak ketat dengan vendor (PDPA *Section* 26, *Guide Part* III)
Sanksi Pelanggaran	Sanksi pidana penjara dan denda hingga Rp6 miliar (UU PDP Pasal 67-68)	Denda administratif hingga SGD 1 juta (PDPA *Section* 29)
Pendekatan Regulasi	Pendekatan prosedural dan eksplisit, mengutamakan kepastian hukum dan persetujuan eksplisit	Pendekatan berbasis risiko dan prinsip, memberikan fleksibilitas dalam penerapan perlindungan

2. Studi Kasus Worldcoin dalam Konteks Regulasi Perlindungan Data Biometrik

Program *Worldcoin*, yang menggunakan pemindaian iris untuk memberikan identitas digital global, telah menimbulkan kontroversi di banyak negara karena metode pengumpulan data biometriknya. Di Eropa, proyek ini mendapat tantangan hukum yang signifikan dari beberapa otoritas perlindungan data, seperti di Prancis dan Jerman. Otoritas Perlindungan Data Bavaria, yang bertindak untuk *Worldcoin Foundation* yang berbasis di Jerman, menyatakan sedang melakukan investigasi mendalam terhadap legalitas pengumpulan data biometrik *Worldcoin* di bawah *General Data Protection Regulation* (GDPR).[17] GDPR mewajibkan dasar hukum yang kuat, termasuk informed consent yang sah, untuk pengolahan data sensitif seperti biometrik (GDPR *Article 9*).[18] Investigasi ini mencerminkan prinsip kehati-hatian tinggi Eropa terhadap teknologi pengumpulan identitas berbasis biometrik.

Berbeda dengan Eropa, Singapura menanggapi program Worldcoin dengan pendekatan regulasi yang berbasis prinsip. Otoritas Perlindungan Data Singapura (*Personal Data Protection Commission/PDPC*) menyatakan pihaknya telah memulai penyelidikan terhadap operasi Worldcoin di Singapura. Namun, hingga saat ini belum ada keputusan pembekuan atau pelarangan resmi.[19] Dalam kerangka PDPA Singapura, data biometrik seperti iris termasuk kategori sensitive personal data,

[17] Reuters, *Worldcoin must delete all iris scan data, watchdog says*, 2024, https://www.reuters.com/markets/currencies/spanish-watchdog-tells-worldcoin-delete-all-iris-scan-data-2024-12-19/

[18] Edward S. Dove, What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e), *International Data Privacy Law*, Vol 11, No 2, 2021, hlm. 107

[19] Masha Borak, *Singaporean regulators zoom in on Worldcoin, 2024*, https://www.biometricupdate.com/202409/singaporean-regulators-zoom-in-on-worldcoin

tetapi penggunaannya bisa dibenarkan tanpa persetujuan eksplisit dalam kondisi tertentu seperti kepentingan sah atau keamanan. Ini tercermin dalam *Guide on Responsible Use of Biometric Data in Security Applications*, yang menguraikan bahwa data biometrik dapat dikumpulkan tanpa persetujuan jika tujuannya sah dan risikonya rendah.

Sementara itu, di Indonesia, proyek Worldcoin dihentikan oleh Kementerian Komunikasi dan Informatika (Kominfo) karena kekhawatiran akan perlindungan data pribadi. Pemindaian iris dilakukan di sejumlah wilayah seperti Jakarta, Bandung, dan Tangerang, sebelum kemudian dibekukan sementara pada Mei 2025. Menurut juru bicara Kominfo, penghentian ini dilakukan karena belum ada kejelasan mengenai cara penyimpanan, pemrosesan, dan transfer data biometrik warga ke luar negeri.[20] Keputusan ini menunjukkan bahwa meskipun Indonesia telah memiliki Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), ketiadaan otoritas independen seperti PDPC di Singapura membuat penegakan dan evaluasi kebijakan masih bersifat *ad hoc*.

Perbedaan respons antara Eropa, Singapura, dan Indonesia menggarisbawahi perbedaan sistem hukum dan institusi perlindungan data di masing-masing negara. Eropa memiliki kerangka hukum komprehensif seperti GDPR yang tidak hanya menetapkan kewajiban substantif, tetapi juga memiliki otoritas pelaksana independen di setiap negara anggota.[21] Singapura, meskipun tidak menggunakan

[20] Kamila Meilina, *Worldcoin Diblokir, Bagaimana Nasib 500 Ribu Data Iris Mata Warga Indonesia?*, 2025, https://katadata.co.id/digital/teknologi/681d9cdd6c562/worldcoin-diblokir-bagaimana-nasib-500-ribu-data-iris-mata-warga-indonesia?

[21] Yohanes Hermanto Sirait, General Data Protection Regulation (GDPR) Dan Kedaulatan Negara Non-Uni Eropa, *Gorontalo Law Review*, Volume 2 Nomor 2, 2019, hlm. 69

sistem pengawasan yang setajam GDPR, memiliki PDPC yang menjalankan fungsi regulasi berbasis risiko dan prinsip akuntabilitas. Indonesia, di sisi lain, masih dalam tahap transisi dan belum membentuk lembaga otoritas pelindung data pribadi sebagaimana diamanatkan UU PDP (Pasal 58).

Ketidakhadiran otoritas perlindungan data di Indonesia berdampak besar terhadap efektivitas perlindungan warga terhadap penyalahgunaan data biometrik. Hal ini diperparah dengan keterbatasan pengaturan teknis. Misalnya, Permenkumham No. 37 Tahun 2016 memang mengatur standar pengelolaan data biometrik (khususnya sidik jari), tetapi tidak secara eksplisit mencakup data iris. Berbeda dengan Singapura, yang memiliki panduan spesifik tentang penggunaan data iris dalam dokumen teknis mereka, sehingga lembaga atau organisasi dapat mengikuti pedoman teknis berbasis prinsip dan risiko secara langsung.

Kasus *Worldcoin* juga bisa dibandingkan dengan kasus *Clearview AI* di Eropa dan Amerika. *Clearview AI*, sebuah perusahaan pengenal wajah, menghadapi berbagai tuntutan hukum di Eropa karena mengumpulkan data wajah secara masif dari internet tanpa persetujuan. Otoritas Perlindungan Data Inggris (ICO) sempat mengeluarkan denda sebesar £7,5 juta sebelum akhirnya digugat balik oleh Clearview AI.[22] Ini menunjukkan bahwa perusahaan pemroses data biometrik semakin menantang otoritas hukum dengan menyoal batas yurisdiksi dan validitas otorisasi data. Dengan demikian perkembangan teknologi pengenalan

[22] Won Kyung Jung, Privacy and data protection regulations for AI using publicly available data: Clearview AI case, *ICEGOV '24: Proceedings of the 17th International Conference on Theory and Practice of Electronic Governance*, 2024, hlm. 50

biometrik telah menguji batas efektivitas regulasi privasi yang ada.[23]

Respons berbeda ini berdampak langsung pada perlindungan hak warga negara. Di Eropa, warga memiliki hak yang lebih kuat untuk menuntut penghapusan data (*right to be forgotten*) dan pengawasan atas transfer lintas negara.[24] Di Singapura, warga mengandalkan prinsip akuntabilitas dan prosedur keluhan ke PDPC. Di Indonesia, belum ada kanal pengaduan yang terpusat dan bersifat independen, membuat masyarakat lebih rentan terhadap pelanggaran privasi tanpa kompensasi yang jelas.

Penanganan data biometrik oleh *Worldcoin* seharusnya dilihat dalam kerangka prinsip perlindungan data yang berlandaskan data *minimisation* dan *purpose limitation*. Prinsip data *minimisation* menuntut bahwa data pribadi yang dikumpulkan harus sebatas yang diperlukan untuk tujuan yang sah dan spesifik, dan tidak lebih dari itu.[25] Dalam konteks ini, pengumpulan data biometrik yang sangat sensitif seperti iris oleh *Worldcoin* tanpa kejelasan tujuan dan jangka waktu penyimpanan menimbulkan keraguan terhadap kepatuhan terhadap prinsip tersebut. Hal ini menunjukkan potensi pelanggaran prinsip dasar pelindungan data, apalagi dalam yurisdiksi seperti Indonesia yang belum memiliki otoritas pengawas independen.

Selain itu, pendekatan yang berbasis risiko (*risk-based approach*) menjadi sentral dalam diskursus global perlindungan data

[23] Luis Felipe Miranda Ramos, Biometric Technologies and the Law: Developing a Taxonomy for Guiding Policymakers, *A PREPRINT*, 2023, hlm. 8

[24] Uta Kohl, The Right To Be Forgotten In Data Protection Law And Two Western Cultures Of Privacy, *International & Comparative Law Quarterly*, Volume 72 Issue 3, 2023, hlm. 738

[25] Daffa Ladro Kusworo, Conception of An Independent Surveillance Authority in the Effort to Protect Population Data, *Administrative And Environmental Law Review*, Volume 3 Issue 1, 2022, hlm. 14

biometrik. Data biometrik—termasuk data iris—mempunyai tingkat risiko yang tinggi karena sifatnya yang tidak dapat diubah dan bersifat identifikasi permanen.[26] Oleh karena itu, perlindungan hukum atas data jenis ini harus lebih ketat dibanding data lainnya. Negara seperti Singapura telah mengadopsi prinsip ini melalui panduan teknis seperti *Guide on Responsible Use of Biometric Data in Security Applications,* yang menekankan pada mekanisme enkripsi dan segregasi data biometrik dengan data identitas. Sebaliknya, Indonesia belum memiliki panduan teknis sekomprehensif ini, selain yang terbatas pada sidik jari dalam Permenkumham No. 37 Tahun 2016.

Perbandingan antar yurisdiksi ini memperlihatkan bahwa efektivitas perlindungan data biometrik tidak hanya ditentukan oleh kejelasan regulasi, tetapi juga oleh kesiapan institusional dan keberadaan panduan teknis yang kontekstual. Ketika teknologi pengumpulan data biometrik seperti iris scan semakin berkembang dan digunakan secara massal oleh entitas seperti *Worldcoin,* negara-negara perlu menyeimbangkan antara inovasi teknologi dan hak fundamental warga atas privasi. Dengan mengacu pada praktik terbaik dan standar internasional, Indonesia perlu mempercepat pembentukan otoritas pengawas dan menyusun peraturan teknis spesifik untuk jenis biometrik yang lebih kompleks, agar tidak tertinggal dalam perlindungan data di era digital.

F. Penutup/Kesimpulan

Perbandingan antara regulasi perlindungan data pribadi di Indonesia dan Singapura dalam konteks kasus *Worldcoin* menunjukkan adanya perbedaan pendekatan yang signifikan. Indonesia mengadopsi

[26] Idoko Peter Idoko, Big data and AI in employment: The dual challenge of workforce replacement and protecting customer privacy in biometric data usage, *Global Journal of Engineering and Technology Advances*, 19(02), 2024, hlm. 103

model hukum yang lebih prosedural dengan penekanan pada persetujuan eksplisit dan klasifikasi data biometrik sebagai data spesifik, sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022. Namun, kelemahan terletak pada keterbatasan instrumen teknis dan belum terbentuknya otoritas pelindung data independen. Sebaliknya, Singapura melalui *Personal Data Protection Act* (PDPA) dan panduan teknis seperti *Guide on Responsible Use of Biometric Data* mengadopsi pendekatan berbasis prinsip dan risiko, dengan keberadaan *Personal Data Protection Commission* (PDPC) sebagai otoritas pelaksana yang aktif. Keberagaman pendekatan ini berdampak pada tingkat respons negara terhadap kasus seperti Worldcoin, yang melibatkan penggunaan teknologi biometrik canggih seperti pemindaian iris.

Indonesia perlu segera memperkuat kerangka implementasi perlindungan data pribadi dengan membentuk otoritas pengawas yang independen dan menerbitkan regulasi turunan yang lebih teknis, khususnya terkait pemrosesan data biometrik. Selain itu, perlu adanya peningkatan literasi digital masyarakat serta mekanisme pengawasan terhadap aktor global seperti *Worldcoin* yang beroperasi lintas yurisdiksi. Di tengah berkembangnya teknologi pemindaian biometrik yang semakin kompleks, penting bagi Indonesia untuk tidak hanya mengikuti perkembangan global, tetapi juga menyusun kebijakan yang proaktif dan adaptif guna melindungi hak privasi warga negara secara menyeluruh.

Daftar Pustaka

1. Buku

Amar Ahmad, *Perkembangan Teknologi Komunikasi dan Informasi*, Universitas Brawijaya, Jakarta, 2012.

Mukti Fajar dan Yulianto Achmad, *Dualisme Penelitian Hukum Normatif dan Empiris,* Cetakan IV, Pustaka Pelajar, Yogyakarta, 2017.

Satjipto Rahardjo, *Sosiologi Hukum Perkembangan Metode dan Pilihan Masalah*, Penerbit Muhammadiyah, Surakarta, 2004.

Stuart Russell dan Peter Norvig, Artificial Intelligence: A Modern Approach, 4th ed, Pearson, New York, 2021.

Sugiyono, *Memahami Penelitian Kualitatif*, Alfabeta, Bandung, 2012.

2. Artikel Jurnal

Daffa Ladro Kusworo, "Conception of An Independent Surveillance Authority in the Effort to Protect Population Data", *Administrative And Environmental Law Review*, Volume 3, Issue 1, 2022.

Edward S. Dove, "What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e)", *International Data Privacy Law,* Vol. 11, No. 2, 2021.

Fahreddin Sadikoglu, "Biometric Retina Identification Based On Neural Network", *Procedia Computer Science,* Volume 102, 2016.

Gaurav Malik, "Biometric Authentication-Risks And Advancements In Biometric Security Systems", *Journal of Computer Science and Technology Studies*, Vol. 6, No. 3.

Idoko Peter Idoko, "Big data and AI in employment: The dual challenge of workforce replacement and protecting customer privacy in biometric data usage", *Global Journal of Engineering and Technology Advances*, Vol. 19, No. 2, 2024.

Luis Felipe Miranda Ramos, "Biometric Technologies and the Law: Developing a Taxonomy for Guiding Policymakers", *A Preprint*, 2023.

Mauro Barni, "Iris Deidentification With High Visual Realism for Privacy Protection on Websites and Social Networks", *IEEE Access,* Vol. 9, 2021.

Rian Mangapul Sirait, "Tantangan Hukum Penggunaan Data Biometrik dalam Keperluan Bisnis", *Jurnal Konseling Pendidikan Islam,* Vol. 4, No. 2, Juli, 2023.

Sugandha Agarwal, "A Comparative Study of Facial, Retinal, Iris and Sclera Recognition Techniques", *IOSR Journal of Computer Engineering*, Volume 16, Issue 1, 2014.

Uta Kohl, "The Right To Be Forgotten In Data Protection Law And Two Western Cultures Of Privacy", *International & Comparative Law Quarterly,* Volume 72, Issue 3, 2023.

Won Kyung Jung, "Privacy and data protection regulations for AI using publicly available data: Clearview AI case", ICEGOV '24: *Proceedings of the 17th International Conference on Theory and Practice of Electronic Governance*, 2024.

Yohanes Hermanto Sirait, "General Data Protection Regulation (GDPR) Dan Kedaulatan Negara Non-Uni Eropa", *Gorontalo Law Review,* Volume 2, Nomor 2, 2019.

3. Internet

"Diprotes Banyak Negara, Apakah World App Aman?", https://www.medcom.id/teknologi/news-teknologi/JKR5eZVk-diprotes-banyak-negara-apakah-world-app-aman, diakses tanggal 20 Mei 2025.

"Guide on Responsible Use of Biometric Data in Security Applications", https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Guide-on-Responsible-Use-of-Biometric-Data-in-Security-Applications.pdf, diakses tanggal 20 Mei 2025.

"Lockbit 3.0 Diduga Curi Data dan Password 15 Juta Nasabah BSI", https://www.cnnindonesia.com/ekonomi/20230513102703-92-949058/lockbit-30-diduga-curi-data-dan-password-15-juta-nasabah-bsi, diakses tanggal 20 Mei 2025.

"Siaran Pers No. 138/HM/KOMINFO/07/2023 tentang Perkembangan Penanganan Dugaan Kebocoran Data Paspor 34,9 Juta Warga Indonesia", https://www.komdigi.go.id/berita/siaran-pers/detail/siaran-pers-no-138-hm-kominfo-07-2023-tentang-perkembangan-penanganan-dugaan-kebocoran-data-paspor-34-9-juta-warga-indonesia, diakses tanggal 20 Mei 2025.

"Worldcoin must delete all iris scan data, watchdog says", https://www.reuters.com/markets/currencies/spanish-watchdog-tells-worldcoin-delete-all-iris-scan-data-2024-12-19/, diakses tanggal 20 Mei 2025.

Jack Thorne, "Clearview AI Inc v the ICO: Where Technology and Data Protection Collide", https://www.mwe.com/insights/clearview-ai-inc-v-the-ico-where-technology-and-data-protection-collide/, diakses tanggal 20 Mei 2025.

Kamila Meilina, "Worldcoin Diblokir, Bagaimana Nasib 500 Ribu Data Iris Mata Warga Indonesia?", https://katadata.co.id/digital/teknologi/681d9cdd6c562/worldcoin-diblokir-bagaimana-nasib-500-ribu-data-iris-mata-warga-indonesia?, diakses tanggal 20 Mei 2025.

Maria Fransisca Lahur, "Datanya Diduga Dibobol Bjorka, BPJS Malah Dipuji Pakar", https://www.tempo.co/digital/datanya-diduga-dibobol-bjorka-bpjs-malah-dipuji-pakar-208711, diakses tanggal 20 Mei 2025.

Masha Borak, "Singaporean regulators zoom in on Worldcoin", https://www.biometricupdate.com/202409/singaporean-regulators-zoom-in-on-worldcoin, diakses tanggal 20 Mei 2025.

4. Peraturan Perundang-Undangan

Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

Peraturan Menteri Hukum dan HAM Nomor 37 Tahun 2016 Tentang Tata Cara Pengambilan, Perumusan, Dan Identifikasi Teraan Sidik Jari.

Personal Data Protection Act 2012 (PDPA Singapore), Government of Singapore, 2012.

General Data Protection Regulation (GDPR) (EU Regulation 2016/679), European Union, 2016.