Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 1, 2026
DOI: https://doi.org/10.61104/alz.v4i1.3740

Tanggung Jawab Hukum Platform Digital Worldapp Terhadap Pelanggaran Perlindungan Kerahasiaan Data Biometrik Berdasarkan Sistem Hukum Indonesia

I Putu Ayanda Rizki[1], Bagus Gede Ari Rama[2], Ni Putu Sawitri Nandari[3], Komang Satria Wibawa Putra[4]
Program Studi Hukum, Fakultas Hukum, Universitas Pendidikan Nasional, Indonesia[1-4]
Email Korespondensi: kikikayanda@gmail.com, arirama@undiknas.ac.id, sawitrinandari@undiknas.ac.id, komangsatria@undiknas.ac.id

Article received: 01 November 2025, Review process: 11 November 2025
Article Accepted: 25 Desmber 2025, Article published: 12 Januari 2026

ABSTRACT
This research analyzes the legal responsibility of the WorldApp digital platform regarding violations of biometric data confidentiality protection in Indonesia based on Law Number 27 of 2022 concerning Personal Data Protection. The era of digital revolution has brought fundamental transformation in the management of personal data, particularly biometric data which has unique, permanent, and immutable characteristics. The WorldApp case, which offered financial compensation for iris scanning of Indonesian citizens, has raised serious controversy regarding privacy protection and biometric data security. This research employs normative legal research methods with a case study approach to violations committed by WorldApp. The research findings indicate that WorldApp committed various substantive violations of the Personal Data Protection Law, including: violation of registration obligations as an Electronic System Provider, violation of consent principles that do not meet informed consent standards, violation of purpose limitation principles in biometric data collection, violation of data protection and security obligations, and failure to conduct Data Protection Impact Assessment. The qualification of these violations creates administrative, civil, and criminal legal responsibilities for the WorldApp platform. This research contributes to understanding the implementation of the Personal Data Protection Law in facing rapidly developing biometric technology challenges, as well as the importance of strict law enforcement to protect citizens' personal data in the digital era.
Keywords: *Biometric Data, Cybersecurity, Digital Platform*

ABSTRAK
Penelitian ini menganalisis tanggung jawab hukum platform digital WorldApp terhadap pelanggaran perlindungan kerahasiaan data biometrik di Indonesia berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Era revolusi digital telah membawa transformasi fundamental dalam pengelolaan data pribadi, khususnya data biometrik yang memiliki karakteristik unik, permanen, dan tidak dapat diubah. Kasus WorldApp yang menawarkan kompensasi finansial untuk pemindaian iris mata warga negara Indonesia telah menimbulkan kontroversi serius terkait perlindungan privasi dan keamanan data biometrik. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan studi kasus terhadap pelanggaran yang dilakukan oleh WorldApp. Hasil penelitian menunjukkan bahwa WorldApp melakukan berbagai pelanggaran substantif terhadap UU PDP, meliputi: pelanggaran kewajiban pendaftaran sebagai Penyelenggara

Sistem Elektronik, pelanggaran prinsip persetujuan (consent) yang tidak memenuhi standar informed consent, pelanggaran prinsip pembatasan tujuan dalam pengumpulan data biometrik, pelanggaran kewajiban perlindungan dan keamanan data, serta kegagalan melaksanakan Penilaian Dampak Perlindungan Data Pribadi (Data Protection Impact Assessment). Kualifikasi pelanggaran-pelanggaran ini menciptakan tanggung jawab hukum baik administratif, perdata, maupun pidana bagi platform WorldApp. Penelitian ini memberikan kontribusi pemahaman mengenai implementasi UU PDP dalam menghadapi tantangan teknologi biometrik yang berkembang pesat, serta pentingnya penegakan hukum yang tegas untuk melindungi data pribadi warga negara di era digital.
Kata Kunci: *Data Biometrik, Keamanan Siber, Platform Digital*

PENDAHULUAN

Era revolusi digital telah membawa transformasi fundamental dalam berbagai aspek kehidupan manusia, termasuk dalam hal pengelolaan dan pemanfaatan data pribadi. Di Indonesia, perkembangan teknologi digital telah menciptakan peluang sekaligus tantangan baru dalam perlindungan kerahasiaan data pribadi, khususnya data biometrik yang memiliki karakteristik unik dan tidak dapat diubah. Data pribadi mencakup setiap informasi yang dapat digunakan untuk mengidentifikasi atau menghubungi individu tertentu, baik informasi tersebut dikumpulkan secara langsung atau tidak langsung melalui metode elektronik dan/atau non-elektronik. Perkembangan teknologi biometrik dalam platform digital telah menciptakan paradigma baru dalam identifikasi dan autentikasi digital. Data biometrik, yang meliputi sidik jari, pemindaian wajah, pemindaian iris mata, dan karakteristik fisik lainnya, memiliki keunikan tersendiri karena sifatnya yang permanen dan tidak dapat diubah. Hal ini berbeda dengan data pribadi konvensional seperti kata sandi atau PIN yang dapat dimodifikasi jika terjadi kebocoran. Karakteristik khusus inilah yang membuat data biometrik memerlukan perlindungan hukum yang lebih ketat dan komprehensif. Dalam konteks global, pemanfaatan data biometrik untuk keperluan identifikasi digital telah menjadi tren yang semakin berkembang. Platform-platform teknologi besar mulai mengintegrasikan sistem biometrik untuk meningkatkan keamanan dan kemudahan akses bagi pengguna. Namun, pemanfaatan teknologi ini juga menimbulkan kekhawatiran serius terkait privasi dan keamanan data pribadi, terutama dalam hal pengumpulan, pengolahan, penyimpanan, dan penggunaan data biometrik oleh pihak ketiga (Anggen Suari & Sarjana, 2023; Dhianty, 2022).

Indonesia telah memiliki kerangka hukum yang relatif komprehensif dalam mengatur perlindungan data pribadi, yang dimulai dengan pengakuan hak atas privasi sebagai hak konstitusional dalam Undang-Undang Dasar 1945. Undang-Undang Dasar 1945 Republik Indonesia menetapkan hak atas privasi sebagai hak dasar warga negara, yang kemudian menjadi fondasi bagi pengembangan regulasi yang lebih spesifik dalam bidang perlindungan data pribadi. Tonggak penting dalam perlindungan data pribadi di Indonesia adalah disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini merupakan respons terhadap kebutuhan mendesak akan perlindungan data pribadi di era digital yang semakin kompleks. Menurut informasi yang dimuat

dalam Klinik Hukumonline, 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. Kompleksitas hukum semakin meningkat ketika platform digital beroperasi secara transnasional namun mengumpulkan data dari warga negara Indonesia, menciptakan pertanyaan mendasar tentang yurisdiksi, subjek hukum yang bertanggung jawab, dan mekanisme penegakan hukum yang efektif. Pengalaman dalam pengaturan teknologi baru seperti AI menunjukkan bahwa kecepatan adaptasi regulasi menjadi faktor krusial dalam memastikan perlindungan hukum yang memadai bagi masyarakat, terutama mengingat karakteristik data biometrik yang bersifat permanen dan tidak dapat dipulihkan jika terjadi kebocoran atau penyalahgunaan (Aruan, 2024; Fitria et al., 2025).

Data biometrik memiliki karakteristik unik yang membedakannya dari data pribadi konvensional. Keunikan ini terletak pada sifatnya yang permanen, tidak dapat diubah, dan sangat personal. Berbeda dengan kata sandi atau PIN yang dapat diganti jika terjadi kebocoran, data biometrik seperti sidik jari, pemindaian iris mata, atau geometri wajah tidak dapat dimodifikasi. Karakteristik ini menciptakan risiko yang lebih tinggi jika terjadi kebocoran atau penyalahgunaan data. Dalam konteks hukum Indonesia, data biometrik dikategorikan sebagai data pribadi yang bersifat spesifik dan memerlukan perlindungan khusus. Menurut analisis yang dimuat dalam publikasi hukum terkini, data biometrik termasuk dalam kategori data pribadi yang sangat sensitif dan dilindungi secara khusus oleh Undang-Undang Perlindungan Data Pribadi . Perlindungan khusus ini mencakup persyaratan yang lebih ketat dalam hal persetujuan, pengolahan, penyimpanan, dan penggunaan data. Implementasi desain privasi (privacy by design) menjadi aspek krusial dalam perlindungan data biometrik. Berdasarkan penelitian yang dipublikasikan dalam Veritas et Justitia, implementasi desain privasi sebagai pelindung privasi atas data biometrik harus mempertimbangkan prinsip-prinsip fundamental seperti minimalisasi data, pembatasan tujuan, dan transparansi dalam pengolahan data (Gede Ari Rama et al., 2023; Hanaya, 2023; Jain, 2025).

Platform WorldApp, yang merupakan bagian dari ekosistem Worldcoin, telah menjadi sorotan publik global, termasuk di Indonesia, karena pendekatan uniknya dalam mengumpulkan data biometrik pengguna. Aplikasi ini menawarkan kompensasi finansial kepada pengguna yang bersedia memindai iris mata mereka untuk keperluan verifikasi identitas digital. Popularitas WorldApp meningkat pesat setelah menawarkan imbalan berupa mata uang kripto kepada pengguna yang berpartisipasi dalam program pemindaian biometrik. Sistem yang ditawarkan oleh WorldApp melibatkan penggunaan perangkat khusus yang disebut "Orb" untuk melakukan pemindaian iris mata pengguna. Proses ini menghasilkan World ID, yang diklaim sebagai identitas digital yang unik dan aman. Menurut informasi yang dimuat dalam Antara News, World ID diperoleh melalui proses pemindaian iris mata yang kemudian dikonversi menjadi kode unik yang dapat digunakan untuk verifikasi identitas anonim di jaringan blockchain (Nur, 2021; Rahman, 2025).

Namun, kehadiran WorldApp di Indonesia telah menimbulkan berbagai kontroversi dan kekhawatiran. Berdasarkan laporan dari berbagai media, aktivitas

pemindaian iris mata dilakukan di berbagai kota seperti Depok dan Bekasi dengan imbalan uang tunai antara Rp 250.000 hingga Rp 800.000 per orang. Aktivitas ini dilakukan tanpa transparansi dan penjelasan yang memadai mengenai risiko jangka panjang terhadap data biometrik warga. Kekhawatiran utama yang muncul adalah terkait dengan keamanan dan privasi data biometrik yang dikumpulkan. Pemerintah Indonesia melalui Kementerian Komunikasi dan Digital (Komdigi) telah merespons dengan tegas terhadap aktivitas WorldApp yang dinilai berpotensi melanggar ketentuan hukum nasional. Berdasarkan evaluasi yang dilakukan, Komdigi menyimpulkan bahwa Tools for Humanity (TFH) selaku pengembang WorldApp dan mitranya belum sepenuhnya memenuhi ketentuan hukum nasional, baik dari aspek perizinan maupun perlindungan data pribadi. Tindakan konkret yang diambil oleh Komdigi adalah membekukan akses terhadap platform WorldApp, World ID, dan layanan terkait Worldcoin di Indonesia (Sembiring et al., 2024; Watkat et al., 2024).

Kasus WorldApp di Indonesia telah mengungkapkan berbagai tantangan dalam implementasi UU PDP, terutama dalam menghadapi inovasi teknologi yang berkembang pesat. Salah satu tantangan utama adalah gap antara perkembangan teknologi dan kesiapan regulasi dalam mengantisipasi model bisnis baru yang berbasis pada pemanfaatan data biometrik. Kecepatan inovasi teknologi yang tidak diimbangi dengan adaptasi regulasi yang memadai dapat menciptakan celah hukum yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Keterbatasan dalam hal sumber daya dan kapasitas institusi pengawas menjadi hambatan dalam memastikan kepatuhan terhadap ketentuan perlindungan data pribadi, terutama untuk platform digital yang beroperasi secara global . Aspek yurisdiksi juga menjadi tantangan kompleks dalam kasus WorldApp. Platform ini dikembangkan oleh entitas yang berbasis di luar Indonesia namun beroperasi dan mengumpulkan data dari warga negara Indonesia. Hal ini menciptakan kompleksitas dalam hal penentuan yurisdiksi hukum yang berlaku dan mekanisme penegakan hukum yang efektif. Prinsip territorial dan personal jurisdiction menjadi pertimbangan penting dalam menentukan kewenangan hukum Indonesia dalam mengatur platform digital asing. Tantangan lain yang tidak kalah penting adalah edukasi dan kesadaran masyarakat terhadap risiko yang terkait dengan pemberian data biometrik. Kurangnya pemahaman masyarakat mengenai implikasi jangka panjang dari pemberian data biometrik dapat menjadi celah yang dimanfaatkan oleh platform yang tidak bertanggung jawab. Sebagaimana ditekankan dalam berbagai publikasi hukum, masyarakat perlu diberikan edukasi yang memadai mengenai hak-hak mereka dalam hal perlindungan data pribadi dan cara melindungi diri dari potensi penyalahgunaan data.

METODE

Penelitian ini diklasifikasikan sebagai penelitian hukum normatif melalui pendekatan studi kasus normatif yang berfokus pada produk perilaku hukum, khususnya peraturan perundang-undangan. Objek kajian diarahkan pada hukum yang dipahami sebagai norma atau kaidah yang berlaku dalam kehidupan bermasyarakat dan dijadikan pedoman dalam bertindak. Oleh karena itu, dalam

penelitian hukum normatif, perhatian dipusatkan pada penelaahan hukum positif, asas dan doktrin hukum, proses penemuan hukum dalam perkara in concreto, sistematika hukum, tingkat sinkronisasi peraturan, perbandingan hukum, serta perkembangan sejarah hukum.

HASIL DAN PEMBAHASAN

Tanggung Jawab Hukum Platform Digital Terhadap Pelanggaran Perlindungan Kerahasiaan Data Biometrik Berdasarkan Sistem Hukum Indonesia

WorldApp di Indonesia menjadi salah satu contoh paling aktual dan kontroversial mengenai pelanggaran perlindungan data biometrik dalam beberapa tahun terakhir. Pada Mei 2025, WorldApp menjadi sorotan publik karena menawarkan imbalan finansial sebesar Rp800.000 kepada masyarakat Indonesia yang bersedia melakukan pemindaian iris mata mereka, yang kemudian memicu respons cepat dari pemerintah melalui Kementerian Komunikasi dan Digital (Komdigi) dengan membekukan sementara operasional aplikasi tersebut karena diduga belum terdaftar sebagai Penyelenggara Sistem Elektronik (PSE) sesuai ketentuan hukum yang berlaku . Sanksi yang dijatuhkan berupa penghentian sementara seluruh aktivitas pengumpulan dan pemrosesan data iris mata Warga Negara Indonesia, termasuk data yang sebelumnya telah dikumpulkan, dengan kewajiban penghapusan data tersebut. Implementasi kebijakan sering bertentangan dengan harapan, sehingga memerlukan pemahaman mendalam dari perspektif politik (pertarungan kepentingan publik) dan administratif (sistem dan kemampuan pejabat) (Simanjuntak, 2017; Zahra et al., 2024).

Kualifikasi Pelanggaran Worldapp Terhadap Perlindungan Data Biometrik

Untuk menentukan tanggung jawab hukum WorldApp, langkah pertama yang harus dilakukan adalah mengkualifikasi perbuatan-perbuatan WorldApp yang dapat dikategorikan sebagai pelanggaran terhadap ketentuan perlindungan data pribadi di Indonesia. Kualifikasi ini penting karena menentukan dasar hukum dan bentuk tanggung jawab yang dapat dibebankan kepada platform tersebut.

Pelanggaran Kewajiban Pendaftaran sebagai Penyelenggara Sistem Elektronik

Pelanggaran pertama dan paling mendasar yang dilakukan oleh WorldApp adalah tidak terdaftar sebagai Penyelenggara Sistem Elektronik (PSE) sebagaimana diamanatkan dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Kewajiban pendaftaran PSE bukan sekadar formalitas administratif, melainkan mekanisme kontrol dan pengawasan pemerintah terhadap platform digital yang beroperasi di Indonesia, khususnya yang memproses data pribadi warga negara Indonesia . Melalui pendaftaran PSE, pemerintah dapat memastikan bahwa platform digital memenuhi standar keamanan data, memiliki server atau data center di Indonesia untuk data pribadi tertentu, serta tunduk pada yurisdiksi hukum Indonesia. Dalam konteks WorldApp yang mengumpulkan data biometrik berupa pemindaian iris mata, kewajiban pendaftaran PSE menjadi semakin krusial mengingat sensitivitas data yang diproses. Pasal 15 ayat (1) PP 71 Tahun 2019 tentang Penyelenggaraan Sistem

dan Transaksi Elektronik mengatur kewajiban Penyelenggara Sistem Elektronik (PSE) untuk menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan atas permintaan orang yang bersangkutan (right to erasure), yang mencakup penghapusan data dan pengeluaran dari mesin pencari (delisting). Ini adalah hak privasi individu untuk meminta data pribadinya dihapus dari sistem elektronik yang dikelol. Kegagalan WorldApp untuk memenuhi kewajiban ini menunjukkan ketidakpatuhan terhadap regulasi dasar yang mengatur operasi platform digital di Indonesia, yang dengan sendirinya menciptakan tanggung jawab hukum baik administratif maupun pidana (Christian & Christian, 2022; Wahyuanto, 2025).

Pelanggaran Prinsip Persetujuan (Consent) dalam Pemrosesan Data Biometrik

Pelanggaran substantif yang sangat serius dilakukan oleh WorldApp adalah terkait dengan mekanisme perolehan persetujuan (consent) dari subjek data sebelum melakukan pemindaian iris mata. Pasal 20 ayat (2) huruf a UU PDP secara tegas menyatakan bahwa persetujuan yang sah secara eksplisit dari Subjek Data Pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan oleh Pengendali Data Pribadi kepada Subjek Data Pribadi. Lebih lanjut, Pasal 22 ayat (1) UU PDP mengatur bahwa Persetujuan pemrosesan Data Pribadi dilakukan melalui persetujuan tertulis atau terekam. Konsep informed consent dalam konteks data biometrik memiliki makna yang sangat mendalam dan tidak dapat dipandang sekadar sebagai persetujuan formal . Informed consent mengharuskan subjek data untuk benar-benar memahami implikasi dari penyerahan data biometrik mereka, termasuk bagaimana data akan digunakan, siapa yang akan mengaksesnya, berapa lama data akan disimpan, ke mana data akan ditransfer, risiko apa yang mungkin timbul dari kebocoran data, dan hak-hak apa yang dimiliki subjek data. Dalam kasus WorldApp, terdapat keraguan serius apakah pengguna yang tertarik dengan iming-iming uang Rp800.000 benar-benar memahami implikasi jangka panjang dari penyerahan data iris mata mereka . Lebih jauh lagi, Pasal 3 huruf d UU PDP dimana menjelaskan Undang-Undang ini berasaskan asas kemanfaatan yang dimaksud dengan "asas kemanfaatan" adalah bahwa pengaturan Perlindungan Data Pribadi harus bermanfaat bagi kepentingan nasional, khususnya dalam kesejahteraan umum. Namun, aktivitas WorldApp yang mengumpulkan data biometrik untuk tujuan komersial berupa pembangunan sistem identitas digital global tidak masuk dalam kategori pengecualian tersebut, sehingga persetujuan eksplisit mutlak diperlukan. Kegagalan memenuhi standar informed consent ini merupakan pelanggaran yang menciptakan tanggung jawab hukum baik secara perdata maupun administratif bagi WorldApp.

Pelanggaran Prinsip Pembatasan Tujuan (Purpose Limitation)

Prinsip fundamental dalam perlindungan data pribadi adalah prinsip pembatasan tujuan, yang mengharuskan bahwa data pribadi hanya dapat dikumpulkan untuk tujuan yang spesifik, eksplisit, dan legitimate, serta tidak boleh diproses lebih lanjut untuk tujuan yang tidak sesuai dengan tujuan awal pengumpulan. Pasal 4 ayat (1) huruf a UU PDP menjelaskan bahwa Data Pribadi

yang bersifat spesifik merupakan Data Pribadi yang apabila dalam pemrosesannya dapat mengakibatkan dampak lebih besar kepada Subjek Data Pribadi, antara lain tindakan diskriminasi dan kerugian yang lebih besar Subjek Data Pribadi. Pengendali data pribadi harus melakukan pemrosesan data pribadi sesuai dengan tujuan yang telah disampaikan kepada subjek data pribadi pada saat memperoleh persetujuan. Dalam kasus WorldApp, terdapat ketidakjelasan dan potensi pelanggaran serius terhadap prinsip pembatasan tujuan. Platform ini mengumpulkan data iris mata dengan tujuan yang dinyatakan adalah untuk membangun sistem identitas digital global yang dapat memverifikasi keunikan manusia (proof of personhood) dalam menghadapi ancaman kecerdasan buatan dan bot. Namun, terdapat kekhawatiran bahwa data biometrik yang dikumpulkan dapat digunakan untuk tujuan-tujuan lain yang tidak diungkapkan kepada pengguna, seperti pengembangan algoritma pengenalan wajah, penelitian tentang pola biometrik populasi tertentu, atau bahkan penjualan data kepada pihak ketiga untuk keperluan komersial lainnya . Dalam konteks WorldApp yang mengumpulkan data biometrik warga negara Indonesia untuk keperluan sistem identitas global yang berbasis blockchain dan cryptocurrency, terdapat pertanyaan mendasar apakah tujuan tersebut legitimate menurut hukum Indonesia. Sistem yang dibangun oleh WorldApp menggunakan teknologi blockchain yang terdesentralisasi, yang berarti data biometrik warga negara Indonesia akan tersimpan dalam infrastruktur global yang tidak sepenuhnya berada di bawah kendali yurisdiksi Indonesia (Fadilah & Putri, 2025).

Pelanggaran Kewajiban Perlindungan dan Keamanan Data

Kewajiban mendasar setiap pengendali data pribadi adalah memastikan perlindungan dan keamanan data pribadi yang diproses. Pasal 38 UU PDP mengatur bahwa Pengendali Data Pribadi wajib melindungi Data Pribadi dari pemrosesan yang tidak sah.. Kewajiban ini mewajibkan pengendali data pribadi dan prosesor data pribadi untuk melaksanakan sertifikasi, audit keamanan data pribadi secara berkala, serta melaksanakan langkah-langkah teknis dan organisasional yang sesuai untuk melindungi data pribadi. Untuk data biometrik yang memiliki karakteristik unik dan permanen, standar keamanan yang dituntut jauh lebih tinggi dibandingkan data pribadi umum. Data biometrik tidak dapat "diubah" jika terjadi kebocoran seperti halnya password atau PIN, sehingga kebocoran data biometrik menciptakan risiko seumur hidup bagi subjek data. Oleh karena itu, platform yang memproses data biometrik wajib menerapkan state-of-the-art security measures yang mencakup enkripsi end-to-end, penyimpanan data dalam format yang tidak dapat di-reverse engineer kembali ke data mentah (irreversible hashing), kontrol akses yang sangat ketat dengan multi-factor authentication, monitoring real-time terhadap aktivitas mencurigakan, dan mekanisme respons insiden yang cepat dan efektif . Meskipun WorldApp mengklaim menggunakan teknologi blockchain yang terdesentralisasi dan bahwa data biometrik tidak disimpan dalam bentuk mentah melainkan dikonversi menjadi IrisCode yang unik, terdapat pertanyaan tentang apakah langkah-langkah ini cukup untuk memenuhi standar perlindungan data biometrik yang dituntut oleh UU PDP. Penggunaan teknologi blockchain sendiri tidak secara

otomatis menjamin keamanan data, karena terdapat berbagai risiko spesifik yang terkait dengan teknologi ini, seperti immutability yang berarti data yang sudah masuk ke blockchain tidak dapat dihapus sepenuhnya, risiko kompromi private keys yang memberikan akses permanen ke data, serta potensi vulnerabilities dalam smart contracts yang mengelola data. Pengendali data pribadi wajib memberitahu secara tertulis kepada subjek data pribadi paling lambat tiga hari kerja sejak mengetahui terjadinya kegagalan perlindungan data pribadi, dan kepada lembaga pelindungan data pribadi paling lambat tiga hari kerja setelah pemberitahuan kepada subjek data pribadi. Kewajiban breach notification ini sangat penting untuk memberikan kesempatan kepada subjek data untuk mengambil langkah-langkah mitigasi secepatnya. Dalam konteks WorldApp yang mengumpulkan data biometrik puluhan ribu warga Indonesia, kemampuan platform untuk mendeteksi breach dan melakukan notifikasi tepat waktu menjadi pertanyaan krusial, mengingat platform ini bahkan tidak terdaftar sebagai PSE dan tidak memiliki kantor atau perwakilan resmi di Indonesia yang dapat dihubungi yang dimana menjadi tantangan dalam penyelesaiannya. Di Indonesia, platform digital yang menggunakan teknologi finansial juga menghadapi tantangan serupa dalam perlindungan data pribadi, sebagaimana diidentifikasi dalam penelitian tentang fintech peer to peer lending yang menunjukkan kompleksitas hubungan hukum antara para pihak .

Pelanggaran Kewajiban Pelaksanaan Penilaian Dampak Perlindungan Data Pribadi (Data Protection Impact Assessment)

Pasal 34 ayat (1) UU PDP mengatur bahwa Pengendali Data Pribadi wajib melakukan penilaian dampak Pelindungan Data Pribadi dalam hal pemrosesan Data Pribadi memiliki potensi risiko tinggi terhadap Subjek Data Pribadi. Dalam hal ini pengendali data pribadi wajib melaksanakan Penilaian Dampak Perlindungan Data Pribadi (Data Protection Impact Assessment atau DPIA) sebelum melakukan pemrosesan data pribadi yang menimbulkan risiko tinggi terhadap data pribadi. Pemrosesan data pribadi yang menimbulkan risiko tinggi mencakup, antara lain, pemrosesan data pribadi spesifik termasuk data biometrik, pemrosesan data pribadi dalam skala besar, dan pemrosesan data pribadi yang menggunakan teknologi baru. Aktivitas WorldApp memenuhi seluruh kriteria pemrosesan berisiko tinggi yang mensyaratkan pelaksanaan DPIA. Pertama, WorldApp memproses data biometrik berupa pemindaian iris mata yang merupakan data pribadi spesifik dengan tingkat sensitivitas tertinggi. Kedua, WorldApp mengumpulkan data dalam skala masif, tidak hanya di Indonesia tetapi di berbagai negara di dunia, dengan target mengumpulkan data miliaran manusia. Ketiga, WorldApp menggunakan teknologi baru berupa kombinasi biometric scanning, blockchain, dan zero-knowledge cryptography yang belum teruji secara luas dalam konteks perlindungan data pribadi . Tidak ada bukti bahwa WorldApp telah melaksanakan DPIA yang comprehensive sebelum meluncurkan operasinya di Indonesia. Kegagalan melaksanakan DPIA merupakan pelanggaran serius terhadap UU PDP yang menciptakan tanggung jawab hukum administratif. Lebih dari itu, ketiadaan DPIA menunjukkan bahwa WorldApp tidak melakukan due diligence yang memadai

dalam menilai risiko pemrosesan data biometrik warga Indonesia, yang dapat menjadi dasar untuk menetapkan tanggung jawab berdasarkan kelalaian.

Bentuk-Bentuk Tanggung Jawab Hukum Platform Digital dalam Pelanggaran Perlindungan Data Biometrik:

Tanggung Jawab Administratif

Sanksi administratif yang dapat dikenakan mencakup spektrum yang luas, mulai dari peringatan tertulis hingga penghentian sementara kegiatan pemrosesan Data Pribadi. Pasal 57 ayat (2) UU PDP mengatur bahwa sanksi administratif dapat berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan Data Pribadi, penghapusan atau pemusnahan Data Pribadi, dan denda administratif. Sanksi ini dirancang untuk memberikan fleksibilitas kepada lembaga pengawas dalam menyesuaikan tingkat sanksi dengan tingkat keseriusan pelanggaran yang dilakukan. Dalam kasus WorldApp, Kementerian Komunikasi dan Digital telah menerapkan sanksi berupa pembekuan sementara operasional aplikasi berdasarkan temuan bahwa platform belum terdaftar sebagai Penyelenggara Sistem Elektronik dan mengumpulkan data biometrik tanpa memenuhi persyaratan hukum.

Tanggung Jawab Perdata

Tanggung jawab perdata dalam konteks pelanggaran perlindungan data biometrik mengacu pada kewajiban platform digital untuk memberikan ganti rugi kepada subjek data yang mengalami kerugian akibat pelanggaran tersebut. Dasar hukum tanggung jawab perdata ini dapat ditemukan dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata) mengenai perbuatan melawan hukum, yang menyatakan bahwa setiap perbuatan melawan hukum yang membawa kerugian kepada orang lain mewajibkan orang yang karena salahnya menerbitkan kerugian itu untuk mengganti kerugian tersebut. Dalam kasus WorldApp, dasar gugatan mencakup pengumpulan data tanpa informed consent yang sah, kegagalan memberikan informasi memadai tentang tujuan dan mekanisme penyimpanan data, serta penggunaan data untuk tujuan yang tidak disetujui subjek data.

Tanggung Jawab Pidana

Tanggung jawab pidana merupakan bentuk pertanggungjawaban yang paling berat dalam sistem hukum Indonesia, karena tidak hanya mengakibatkan sanksi berupa denda finansial tetapi juga dapat mengakibatkan sanksi penjara bagi pelaku pelanggaran. UU PDP mengatur berbagai ketentuan pidana yang dapat dikenakan kepada pihak-pihak yang melanggar ketentuan perlindungan data pribadi, dengan gradasi sanksi yang disesuaikan dengan tingkat keseriusan pelanggaran. Pasal 67 ayat (1) UU PDP mengatur sanksi pidana bagi setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi. Sanksi yang diancamkan adalah pidana penjara paling lama 5 tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). Dalam konteks

WorldApp, ketentuan ini sangat relevan karena platform tersebut mengumpulkan data biometrik warga negara Indonesia tanpa memenuhi persyaratan hukum yang berlaku dan dengan tujuan komersial berupa pembangunan sistem identitas digital global yang menguntungkan pengembang platform.

SIMPULAN

Penelitian ini mengungkapkan bahwa platform digital WorldApp telah melakukan pelanggaran serius terhadap ketentuan perlindungan data pribadi di Indonesia, khususnya dalam pengumpulan data biometrik berupa pemindaian iris mata warga negara. Pelanggaran-pelanggaran tersebut mencakup kegagalan memenuhi kewajiban pendaftaran sebagai Penyelenggara Sistem Elektronik, tidak terpenuhinya standar informed consent dalam memperoleh persetujuan dari subjek data, pelanggaran prinsip pembatasan tujuan dalam pengumpulan data, ketidakmampuan menjamin keamanan dan perlindungan data biometrik, serta kelalaian dalam melaksanakan Penilaian Dampak Perlindungan Data Pribadi sebagaimana diamanatkan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Kualifikasi pelanggaran-pelanggaran ini menciptakan tanggung jawab hukum berlapis bagi WorldApp, meliputi tanggung jawab administratif berupa sanksi pembekuan operasional dan potensi denda administratif, tanggung jawab perdata berdasarkan prinsip perbuatan melawan hukum yang mewajibkan ganti rugi kepada subjek data yang dirugikan, serta tanggung jawab pidana dengan ancaman sanksi penjara dan denda finansial yang signifikan. Kasus WorldApp mendemonstrasikan urgensi penegakan hukum yang tegas terhadap platform digital yang mengeksploitasi data biometrik warga negara tanpa memenuhi standar perlindungan yang memadai, sekaligus menggarisbawahi pentingnya harmonisasi regulasi nasional dalam menghadapi tantangan teknologi yang beroperasi secara transnasional.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada Universitas Pendidikan Nasional Denpasar yang telah memberikan dukungan penuh dalam pelaksanaan pembuatan jurnal penelitian ini. Tidak lupa ucapan terima kasih kepada dosen pembimbing Bapak Bagus Gede Ari Rama S.H., M.H. yang telah memberikan arahan dan bimbingan selama pelaksanaan pembuatan jurnal penelitian ini. Serta Ibu Ni Putu Sawitri Nandari, S.H. M.H., dan Bapak Dr. Komang Satria Wibawa Putra S.H., M.H. yang telah membantu memberikan saran yang positif.

DAFTAR RUJUKAN

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142.

Aruan, J. E. S. (2024). Perlindungan Data Pribadi Ditinjau Dari Teori Perlindungan Hukum Dan Teori Perlindungan Hak Atas Privasi. *Jurnal Globalisasi Hukum*, *1*(1), 1–22.

Christian, S. H., & Christian, D. (2022). *UU PDP: Landasan Hukum Pelindungan Data*

Pribadi. https://www.hukumonline.com/klinik/a/uu-pdp--landasan-hukum-pelindungan-data-pribadi-lt5d588c1cc649e/

Dhianty, R. (2022). Kebijakan Privasi Dan Peraturan Perundang-Undangan Sektoral Platform Digital Vis a Vis Kebocoran Data Pribadi. *Scripta: Jurnal Kebijakan Publik Dan Hukum*, *2*(1), 186. http://journal.puskapkum.org/index.php/scripta

Fadilah, R., & Putri, M. R. D. (2025). *10 Negara Yang Melarang Scan Biometrik Worldcoin World App*. https://www.antaranews.com/berita/4816969/10-negara-yang-melarang-scan-biometrik-worldcoin-world-app

Fitria, M. et al. (2025). Perlindungan Dan Tanggung Jawab Hukum Kebocoran Informasi Data Pribadi Pada Penyelenggara Sistem Elektronik Berdasarkan Perspektif Rahasia Dagang. *Cerdika: Jurnal Ilmiah Indonesia*, *5*(1), 1416–1423.

Gede Ari Rama, B. et al. (2023). Urgensi Pengaturan Artificial Intelligence Dalam Bidang Hukum Hak Cipta Di Indonesia. *Jurnal Rechtens*, *12*(2), 209–224.

Hanaya, E. (2023). Perlindungan Data Pribadi Di Era Digital Dalam Perspektif Perbandingan Hukum. *Jurnal Bevinding Fakultas Hukum Universitas Islam Batik Surakarta*, *1*(9), 11.

Jain, A. K. (2025). *Introduction to Biometrics*. Springer International Publishing. https://link.springer.com/10.1007/978-3-031-61675-4

Nur, S. (2021). *Buku Pengantar Penelitian Hukum*. CV. Penerbit Qiara Media.

Rahman, T. A. (2025). Polemik Etika Dan Privasi Dalam Pengumpulan Data Biometrik World App. *TEKNOBIS: Jurnal Teknologi, Bisnis Dan Pendidikan*, *3*(2), 250–253.

Sembiring, P. E. et al. (2024). Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik. *Veritas et Justitia*, *10*(1), 127–152.

Simanjuntak, Y. (2017). *Hubungan Adiksi Internet Dengan Ansietas Pada Mahasiswa Fakultas Kedokteran Universitas Sumatera Utara* [Universitas Sumatera Utara]. https://repositori.usu.ac.id/123456789/4598

Wahyuanto, E. (2025). *Pembekuan Worldcoin, WorldID Dan Upaya Melindungi Data Pribadi Rakyat*. https://www.komdigi.go.id/berita/artikel/detail/pembekuan-worldcoin-worldid-dan-upaya-melindungi-data-pribadi-rakyat

Watkat, F. X. et al. (2024). Perlindungan Data Pribadi Melalui Penerapan Sistem Hukum Pidana Di Indonesia. *Jurnal Hukum Ius Publicum*, *5*(1), 153.

Zahra, N. et al. (2024). Perlindungan Hukum Teknologi Identitas Digital Melalui Sistem Verifikasi Identitas Berbasis Biometrik. *Jurnal Pemikiran Dan Penelitian Ilmu-Ilmu Sosial, Hukum, Dan Pengajarannya*, *19*(1), 86–98.