

Tinjauan Yuridis Perlindungan Hak Privasi Pengguna terhadap Pemanfaatan Data Biometrik oleh Platform Digital

Roy Andriansah¹, Aturkian Laia²

Ilmu Hukum, Hukum, Universitas Dirgantara Marsekal Suryadarma, Jakarta Timur, Indonesia¹

Ilmu Hukum, Hukum, Universitas Dirgantara Marsekal Suryadarma, Jakarta Timur, Indonesia²

*Email Korespodensi: roy543486@gmail.com

Sejarah Artikel:

Diterima 11-07-2026
Disetujui 17-07-2026
Diterbitkan 19-07-2026

ABSTRACT

The increasing use of biometric authentication technologies, including facial recognition, fingerprint scanning, and iris recognition, has become a common feature of digital platforms for identity verification and service security. Biometric data are classified as specific personal data requiring a higher level of legal protection because they are permanent and cannot be replaced if compromised. This study aims to examine the legal framework, forms of protection, and effectiveness of Indonesian law in safeguarding users' privacy rights concerning the processing of biometric data. This research employs a normative juridical method using statutory and conceptual approaches, analyzed through a prescriptive-qualitative method. The findings indicate that the Personal Data Protection Law classifies biometric data as specific personal data requiring explicit consent and a lawful basis for processing. However, its effectiveness remains constrained by weak regulatory oversight, inconsistent implementation of Data Protection Impact Assessments (DPIAs), and limited public digital literacy, highlighting the need for stronger technical regulations and independent supervisory institutions.

Keywords: *biometric data; privacy rights; personal data protection; digital platforms; Personal Data Protection Law (PDP Law).*

ABSTRAK

Perkembangan teknologi autentikasi berbasis biometrik, seperti pengenalan wajah, sidik jari, dan pemindaian iris, semakin banyak digunakan oleh platform digital untuk verifikasi identitas dan keamanan layanan. Data biometrik termasuk data pribadi spesifik yang memerlukan perlindungan hukum lebih tinggi karena bersifat permanen dan tidak dapat diganti. Penelitian ini bertujuan menganalisis pengaturan hukum, bentuk perlindungan, dan efektivitas kerangka hukum Indonesia terhadap hak privasi pengguna atas pemanfaatan data biometrik. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan konseptual yang dianalisis secara preskriptif-kualitatif. Hasil penelitian menunjukkan bahwa Undang-Undang Pelindungan Data Pribadi telah mengatur data biometrik sebagai data pribadi spesifik yang memerlukan persetujuan eksplisit serta dasar pemrosesan yang sah. Namun, efektivitas perlindungan masih terkendala lemahnya pengawasan, belum optimalnya pelaksanaan DPIA, dan rendahnya literasi digital masyarakat sehingga diperlukan penguatan regulasi teknis serta kelembagaan pengawas independen.

Katakunci: data biometrik; hak privasi; perlindungan data pribadi; platform digital; UU PDP.

PENDAHULUAN

Digitalisasi layanan publik dan komersial telah mendorong adopsi teknologi biometrik secara meluas sebagai instrumen autentikasi dan verifikasi identitas. Fitur pemindaian sidik jari dan pengenalan wajah kini menjadi mekanisme standar untuk membuka kunci perangkat seluler, mengakses aplikasi perbankan digital, melakukan verifikasi pembayaran, hingga proses pendaftaran akun pada berbagai *platform* digital berbasis kecerdasan artifisial. Fenomena ini tidak lepas dari keunggulan teknis biometrik dibandingkan metode autentikasi konvensional berbasis kata sandi (*password*), yaitu tingkat keunikan yang tinggi, kesulitan pemalsuan, serta kenyamanan penggunaan bagi pengguna.

Namun demikian, di balik keunggulan tersebut, data biometrik menyimpan risiko yang jauh lebih besar dibandingkan data pribadi pada umumnya. Berbeda dengan kata sandi atau nomor identitas yang dapat diganti apabila terjadi kebocoran, data *biometric* seperti pola sidik jari, struktur wajah, atau tekstur iris mata melekat secara permanen pada diri seseorang dan tidak dapat “diperbarui” apabila telah disalahgunakan atau bocor ke pihak yang tidak berwenang. Karakteristik inilah yang menjadikan data biometrik digolongkan sebagai data pribadi yang bersifat spesifik (*sensitive personal data*) dalam Pasal 4 ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang menuntut standar perlindungan hukum lebih ketat dibandingkan data pribadi yang bersifat umum.

Kasus dugaan pengumpulan data biometrik berupa pemindaian iris mata oleh *platform* digital global yang menargetkan miliaran pengguna di berbagai negara, termasuk Indonesia, tanpa didahului penilaian dampak pelindungan data yang memadai, menjadi ilustrasi nyata atas kerentanan tersebut. Otoritas terkait di Indonesia bahkan sempat menjatuhkan sanksi administratif berupa penghentian sementara operasional terhadap *platform* yang belum terdaftar sebagai penyelenggara sistem elektronik namun telah mengumpulkan data biometrik penggunanya. Selain itu, teknologi pengenalan wajah yang digunakan untuk kepentingan keamanan publik maupun komersial juga kerap diimplementasikan tanpa persetujuan yang memadai dari individu yang datanya direkam, sehingga menimbulkan potensi pelanggaran terhadap hak atas privasi yang dijamin Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Persoalan tersebut menjadi semakin kompleks mengingat kerangka hukum pelindungan data pribadi di Indonesia meskipun telah diperkuat melalui pengesahan UU PDP pada tahun 2022 masih menyisakan sejumlah kekosongan pengaturan teknis, khususnya terkait standar keamanan spesifik bagi pemrosesan data biometrik, kewajiban audit keamanan sistem yang memproses data biometrik, serta mekanisme pengawasan terhadap penyelenggara *platform* digital lintas batas yang memproses data biometrik warga negara Indonesia dari luar yurisdiksi nasional. Kondisi ini mendorong perlunya kajian yuridis yang komprehensif mengenai pengaturan, bentuk perlindungan, dan efektivitas hukum Indonesia dalam menjamin hak privasi pengguna atas pemanfaatan data biometrik oleh *platform* digital.

Kajian mengenai perlindungan data pribadi dan hak privasi di Indonesia telah berkembang signifikan, terutama pascapengesahan UU PDP. Kusnadi dan Wijaya (2021) mengkaji perlindungan hukum data pribadi sebagai bagian dari hak privasi dan menegaskan bahwa hak atas privasi merupakan hak konstitusional yang dijamin Pasal 28G ayat (1) UUD 1945, sehingga setiap regulasi teknis mengenai data pribadi harus ditafsirkan sebagai instrumen pelaksana hak asasi tersebut. Priliasari (2023) memfokuskan kajiannya pada perlindungan data pribadi konsumen dalam transaksi *e-commerce* dan menemukan bahwa pelaku usaha digital masih belum sepenuhnya memenuhi kewajiban transparansi pemrosesan data sebagaimana disyaratkan peraturan perundang-undangan.

Kajian yang secara spesifik menyoroiti data biometrik dilakukan oleh Rizki dan Salam (2023), yang

meneliti pertanggungjawaban hukum atas pengumpulan data biometrik melalui kecerdasan artifisial tanpa persetujuan pemilik data, dengan menggunakan studi kasus *Clearview AI* di Yunani dan Inggris sebagai pembandingan komparatif. Penelitian tersebut menyimpulkan bahwa ketiadaan persetujuan eksplisit dalam pengumpulan data biometrik menimbulkan tanggung jawab hukum yang dapat dikenakan baik secara administratif maupun perdata terhadap penyelenggara sistem. Adapun kajian mengenai teknologi pengenalan wajah dilakukan oleh Nasakti (2021), yang menganalisis kekosongan hukum (*ius constituendum*) dalam pengaturan *facial recognition technology* di sektor industri dan penegakan hukum Indonesia, serta menyoroti perlunya pembentukan regulasi khusus yang membatasi ruang lingkup penggunaannya.

Penelitian yang lebih mutakhir mengenai tanggung jawab hukum *platform* digital dilakukan dalam studi kasus *WorldApp*, sebuah *platform* yang mengumpulkan data biometrik berupa pemindaian iris mata dalam skala masif di berbagai negara termasuk Indonesia. Studi tersebut menemukan bahwa kegagalan *platform* melaksanakan penilaian dampak perlindungan data pribadi (*Data Protection Impact Assessment/DPIA*) merupakan pelanggaran serius terhadap UU PDP yang berimplikasi pada tanggung jawab hukum administratif, termasuk sanksi penghentian sementara operasional. Sejalan dengan itu, kajian tentang implementasi UU PDP secara umum juga menunjukkan bahwa tantangan penegakan hukum perlindungan data pribadi di Indonesia tidak hanya terletak pada aspek normatif, tetapi juga pada rendahnya literasi digital masyarakat dan lemahnya kesiapan kelembagaan pengawas.

Penelitian-penelitian terdahulu umumnya membahas perlindungan data pribadi secara umum (Kusnadi & Wijaya, 2021; Priliasari, 2023) atau berfokus pada satu jenis teknologi biometrik tertentu, seperti *facial recognition technology* dalam konteks keamanan publik dan penegakan hukum (Nasakti, 2021), tanpa mengaitkannya secara sistematis dengan tanggung jawab hukum *platform* digital komersial sebagai pengendali data. Studi kasus mengenai *WorldApp* memberikan gambaran konkret mengenai penerapan UU PDP terhadap satu *platform* tertentu, tetapi belum menyusun kerangka analisis yang lebih luas mengenai efektivitas keseluruhan sistem hukum Indonesia dalam mengatur berbagai modalitas biometrik sekaligus (sidik jari, wajah, dan iris) yang digunakan lintas sektor *platform* digital. Penelitian ini berupaya mengisi kesenjangan tersebut dengan menyusun analisis yuridis yang mengintegrasikan tiga dimensi sekaligus: pengaturan normatif data biometrik sebagai hak privasi, bentuk-bentuk perlindungan hukum dan tanggung jawab *platform* digital, serta evaluasi efektivitas implementasi kerangka hukum yang ada, sehingga menghasilkan pemetaan yang lebih komprehensif mengenai kesenjangan antara norma dan praktik.

Berdasarkan uraian latar belakang tersebut, penelitian ini merumuskan beberapa permasalahan yang akan dikaji, yaitu bagaimana pengaturan hukum mengenai perlindungan data biometrik sebagai bagian dari hak privasi pengguna di Indonesia, bagaimana bentuk perlindungan hukum terhadap pengguna atas pemanfaatan data biometrik oleh *platform* digital menurut hukum positif Indonesia, serta sejauh mana efektivitas pengaturan hukum dalam menjamin perlindungan hak privasi pengguna terhadap pemanfaatan data biometrik oleh *platform* digital.

Penelitian ini bertujuan untuk menganalisis pengaturan hukum mengenai kedudukan data biometrik sebagai bagian dari hak privasi dalam sistem hukum Indonesia, mengkaji bentuk-bentuk perlindungan hukum beserta tanggung jawab penyelenggara *platform* digital atas pemanfaatan data biometrik pengguna, serta mengevaluasi efektivitas pengaturan hukum yang berlaku sekaligus mengidentifikasi berbagai tantangan dalam implementasinya pada era digital.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum yuridis normatif (*doctrinal legal research*), yaitu penelitian yang mengkaji hukum sebagai kaidah atau norma yang berlaku melalui penelusuran bahan pustaka dan bahan hukum sekunder (Marzuki, 2014). Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), yang dilakukan dengan menelaah peraturan perundang-undangan yang berkaitan dengan perlindungan data pribadi dan transaksi elektronik, serta pendekatan konseptual (*conceptual approach*), yang digunakan untuk menganalisis konsep data biometrik, hak privasi, dan tanggung jawab pengendali data dalam kerangka doktrin hukum perlindungan data pribadi.

Bahan hukum yang digunakan terdiri atas tiga jenis. Bahan hukum primer meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, khususnya Pasal 28G ayat (1); Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi; Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024; Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik; dan Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan sepanjang relevan dengan pemrosesan data biometrik yang berkaitan dengan data kesehatan. Bahan hukum sekunder meliputi buku-buku hukum perlindungan data pribadi, jurnal ilmiah hukum, hasil penelitian, dan karya ilmiah lain yang relevan dengan data biometrik dan tanggung jawab *platform* digital. Bahan hukum tersier berupa kamus hukum dan ensiklopedia yang digunakan untuk memperjelas istilah teknis. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*), sedangkan analisis dilakukan secara kualitatif dengan metode preskriptif, yaitu dengan menginterpretasikan dan mengevaluasi norma hukum yang berlaku untuk merumuskan argumentasi hukum mengenai pengaturan, bentuk perlindungan, dan efektivitas hukum perlindungan data biometrik di Indonesia.

HASIL DAN PEMBAHASAN

1. Konsep Data Biometrik sebagai Bagian dari Data Pribadi yang Bersifat Sensitif

Data biometrik dapat dipahami sebagai data yang dihasilkan dari pengukuran karakteristik fisik, fisiologis, atau perilaku unik seseorang yang dapat digunakan untuk mengidentifikasi atau memverifikasi identitasnya secara khusus, seperti pola sidik jari, struktur wajah, tekstur iris mata, suara, maupun pola gerakan tubuh. Karakteristik biometrik memiliki dua sifat khas yang membedakannya dari data pribadi pada umumnya, yaitu keunikan (*uniqueness*) dan permanensi (*permanence*). Sifat keunikan menjadikan data biometrik sangat efektif sebagai instrumen identifikasi dan autentikasi, karena probabilitas dua individu memiliki karakteristik biometrik yang identik sangat kecil. Sementara itu, sifat permanensi menjadikan data biometrik berbeda secara fundamental dari kredensial autentikasi konvensional, seperti kata sandi atau nomor identifikasi personal, yang dapat diganti sewaktu-waktu apabila terjadi kebocoran atau penyalahgunaan.

Justru karena sifat permanen inilah, kebocoran data biometrik menimbulkan risiko yang jauh lebih serius dan bersifat ireversibel dibandingkan kebocoran data pribadi pada umumnya. Seseorang yang kata sandinya bocor dapat segera menggantinya, tetapi seseorang yang data sidik jari atau data wajahnya bocor tidak dapat “mengganti” wajah atau sidik jarinya, sehingga risiko penyalahgunaan seperti pemalsuan identitas (*identity theft*), akses ilegal terhadap sistem yang menggunakan autentikasi biometrik yang sama, maupun eksploitasi data untuk tujuan pengawasan tanpa persetujuan akan terus membayangi individu tersebut seumur hidup.

Pengakuan atas karakter sensitif data biometrik tersebut tecermin dalam Pasal 4 ayat (2) UU PDP, yang secara eksplisit menggolongkan data dan informasi kesehatan, data biometrik, data genetika, data catatan kejahatan, data anak, data keuangan pribadi, dan/atau data lainnya sesuai ketentuan peraturan perundang-undangan sebagai data pribadi yang bersifat spesifik. Penggolongan ini membawa konsekuensi yuridis penting, yaitu pemrosesan data biometrik menuntut dasar pemrosesan dan mekanisme perlindungan yang lebih ketat dibandingkan data pribadi yang bersifat umum sebagaimana diatur Pasal 4 ayat (1) UU PDP, yang hanya mencakup data seperti nama lengkap, jenis kelamin, dan kewarganegaraan. Konstruksi hukum ini sejalan dengan doktrin perlindungan data pribadi yang berkembang secara global, yang menempatkan data biometrik dalam kategori “*special category of personal data*” yang memerlukan pengamanan berlapis (Rosadi, dalam Priliasari, 2023).

Signifikansi pengaturan ini juga tampak dari perspektif hak asasi manusia. Sebagai bagian dari data pribadi, data biometrik merupakan perwujudan konkret dari hak atas privasi yang dijamin Pasal 28G ayat (1) UUD 1945, yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya. Data biometrik, sebagai representasi digital dari tubuh dan identitas fisik seseorang, berada pada titik pertemuan antara privasi informasional (*informational privacy*) dan privasi jasmani (*bodily privacy*), sehingga pelanggaran terhadapnya berpotensi menimbulkan dampak yang lebih mendalam dibandingkan pelanggaran atas data pribadi yang bersifat administratif semata (Kusnadi & Wijaya, 2021).

2. Praktik Pemanfaatan Data Biometrik oleh Platform Digital

Pemanfaatan data biometrik oleh platform digital di Indonesia telah meluas ke berbagai sektor. Pada sektor perbankan dan layanan keuangan digital, autentikasi biometrik berupa sidik jari dan pengenalan wajah digunakan sebagai mekanisme verifikasi dua faktor (*two-factor authentication*) untuk mengamankan transaksi dan proses pembukaan rekening secara daring melalui prosedur mengenal nasabah elektronik (*electronic know your customer*). Pada sektor telekomunikasi dan layanan publik, teknologi pengenalan wajah dimanfaatkan untuk kepentingan registrasi kartu prabayar dan verifikasi identitas dalam layanan pemerintahan digital. Pada sektor keamanan publik, sejumlah instansi penegak hukum telah menjajaki penggunaan *facial recognition technology* yang terintegrasi dengan basis data kependudukan untuk kepentingan identifikasi dan pengawasan di ruang publik (Nasakti, 2021).

Praktik yang menimbulkan sorotan tajam belakangan ini adalah kemunculan platform digital global berbasis *blockchain* yang mengumpulkan data biometrik berupa pemindaian iris mata sebagai syarat partisipasi dalam skema verifikasi identitas digital dan distribusi aset kripto. Platform semacam ini mengumpulkan data biometrik dalam skala masif, lintas negara, dengan target mencapai miliaran pengguna, sembari menggunakan kombinasi teknologi *biometric scanning*, *blockchain*, dan *zero-knowledge cryptography* yang relatif baru dan belum teruji secara luas dalam konteks perlindungan data pribadi. Otoritas pengawas di Indonesia mencatat bahwa platform tersebut belum terdaftar sebagai penyelenggara sistem elektronik namun telah mengumpulkan data biometrik penggunaanya, sehingga dijatuhi sanksi administratif berupa pembekuan sementara operasional.

Praktik-praktik tersebut memperlihatkan pola umum yang problematis dari perspektif hukum perlindungan data pribadi, yaitu: pertama, pengumpulan data biometrik yang dilakukan tanpa penjelasan yang memadai mengenai tujuan pemrosesan, jangka waktu penyimpanan, dan pihak ketiga yang berpotensi mengakses data tersebut; kedua, penggunaan mekanisme persetujuan yang bersifat formalitas belaka (*checkbox consent*) tanpa memberikan pemahaman substansial kepada pengguna mengenai risiko yang

melekat pada data biometrik yang bersifat permanen; dan ketiga, minimnya transparansi mengenai standar keamanan teknis yang diterapkan untuk melindungi data biometrik dari akses tidak sah, peretasan, maupun kebocoran.

3. Perlindungan Hak Privasi Pengguna terhadap Pengumpulan, Penyimpanan, Pemrosesan, dan Penggunaan Data Biometrik

Kerangka hukum Indonesia menyediakan sejumlah instrumen normatif untuk melindungi hak privasi pengguna dalam setiap tahapan siklus pemrosesan data biometrik, mulai dari pengumpulan hingga penghapusan. Pada tahap pengumpulan, Pasal 20 UU PDP menetapkan bahwa pengendali data pribadi wajib memiliki dasar pemrosesan yang sah, yang salah satunya adalah persetujuan eksplisit dari subjek data untuk satu atau beberapa tujuan tertentu yang telah disampaikan kepada subjek data. Untuk data pribadi yang bersifat spesifik seperti data biometrik, Pasal 21 UU PDP menegaskan bahwa pemrosesan wajib disertai dengan persetujuan eksplisit dan pelaksanaan perlindungan tambahan, mengingat tingkat risiko yang melekat pada data tersebut jauh lebih tinggi dibandingkan data pribadi umum.

Konsep persetujuan eksplisit ini menuntut standar yang lebih tinggi dibandingkan sekadar persetujuan implisit yang lazim ditemukan pada syarat dan ketentuan layanan (*terms of service*) yang jarang dibaca pengguna secara saksama. Persetujuan yang sah menuntut pengungkapan informasi yang jelas mengenai identitas pengendali data, tujuan pemrosesan, jenis data biometrik yang dikumpulkan, jangka waktu penyimpanan, serta hak-hak subjek data, sejalan dengan prinsip keterbukaan (*transparency*) yang menjadi salah satu asas dasar pemrosesan data pribadi. Kegagalan memenuhi standar tersebut, sebagaimana ditemukan dalam kasus *platform* pemindaian iris mata yang beroperasi di Indonesia, berpotensi dikualifikasikan sebagai pemrosesan data biometrik tanpa dasar hukum yang sah.

Pada tahap penyimpanan dan pemrosesan, Pasal 35 dan Pasal 39 UU PDP mewajibkan pengendali data pribadi untuk melindungi dan memastikan keamanan data pribadi yang diprosesnya, termasuk melindungi dari kehilangan, kebocoran, penyalahgunaan, dan akses secara tidak sah. Kewajiban ini diperkuat dengan ketentuan Pasal 34 UU PDP mengenai kewajiban melakukan penilaian dampak perlindungan data pribadi (DPIA) bagi pengendali data yang melakukan pemrosesan data pribadi berisiko tinggi terhadap subjek data, yang secara eksplisit mencakup pemrosesan data pribadi yang bersifat spesifik dalam skala besar. Pemrosesan data biometrik oleh *platform* digital yang beroperasi dengan basis pengguna masif secara normatif termasuk dalam kategori ini, sehingga kewajiban DPIA seharusnya menjadi prasyarat mutlak sebelum peluncuran layanan.

Selain UU PDP, kerangka hukum transaksi elektronik turut memperkuat perlindungan hak privasi pengguna. Pasal 26 ayat (1) UU ITE menegaskan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan, ketentuan yang secara historis telah menjadi rujukan awal bagi pengaturan persetujuan penggunaan data biometrik sebelum lahirnya UU PDP. Adapun PP PSTE memperkuat kewajiban tersebut melalui ketentuan mengenai kewajiban penyelenggara sistem elektronik untuk menjamin keandalan, keamanan, dan tanggung jawab pengoperasian sistem elektronik yang digunakannya, termasuk sistem yang memproses data biometrik pengguna.

Pada tahap penggunaan, hak-hak subjek data yang diatur dalam Pasal 5 hingga Pasal 16 UU PDP, seperti hak untuk mendapatkan informasi mengenai kejelasan identitas, dasar kepentingan hukum, dan tujuan permintaan dan penggunaan data pribadi; hak untuk melengkapi, memperbarui, dan/atau memperbaiki kesalahan data pribadi; hak untuk mengakhiri pemrosesan, menghapus, dan/atau

memusnahkan data pribadi; serta hak untuk menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi, menjadi instrumen yuridis yang dapat digunakan pengguna untuk mengendalikan bagaimana data biometriknya digunakan oleh *platform* digital, termasuk hak untuk menarik kembali persetujuan yang telah diberikan sebelumnya.

4. Tanggung Jawab Penyelenggara Platform Digital atas Penyalahgunaan, Kebocoran, atau Pemrosesan Data Biometrik Tanpa Persetujuan yang Sah

Penyelenggara *platform* digital yang memproses data biometrik menduduki posisi sebagai pengendali data pribadi (*data controller*) sebagaimana dimaksud Pasal 1 angka 4 UU PDP, yaitu pihak yang menentukan tujuan dan melakukan kendali pemrosesan data pribadi. Kedudukan ini membawa konsekuensi tanggung jawab hukum yang melekat sejak tahap perancangan sistem (*privacy by design*) hingga tahap pengoperasian layanan.

Secara administratif, Pasal 57 UU PDP mengatur bahwa pelanggaran terhadap kewajiban pengendali data pribadi dapat dikenakan sanksi administratif berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, dan/atau denda administratif. Ketentuan ini memberikan fleksibilitas bagi otoritas pengawas untuk menyesuaikan bentuk sanksi dengan tingkat keseriusan pelanggaran, sebagaimana tercermin dalam praktik penjatuhan sanksi pembekuan sementara operasional terhadap *platform* yang memproses data biometrik tanpa dasar hukum yang sah dan tanpa terdaftar sebagai penyelenggara sistem elektronik.

Secara perdata, Pasal 12 UU PDP memberikan hak kepada subjek data untuk mengajukan gugatan dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi yang menyimpannya, yang dapat diajukan melalui mekanisme peradilan perdata sesuai hukum acara yang berlaku. Tanggung jawab perdata ini relevan terutama dalam kasus kebocoran data biometrik yang mengakibatkan kerugian materiil maupun immateriil bagi pengguna, seperti penyalahgunaan identitas untuk tindak pidana penipuan atau pengambilalihan akun secara tidak sah menggunakan data biometrik yang dicuri.

Secara pidana, Pasal 67 hingga Pasal 73 UU PDP mengancamkan sanksi pidana penjara dan/atau denda bagi setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya, mengungkapkan data pribadi, atau menggunakan data pribadi yang bukan miliknya, dengan ancaman pidana yang diperberat apabila pelanggaran dilakukan oleh korporasi. Ketentuan ini menempatkan pemrosesan data biometrik tanpa persetujuan yang sah sebagai tindak pidana yang dapat dipertanggungjawabkan baik oleh individu maupun oleh badan hukum penyelenggara *platform* digital, sejalan dengan prinsip pertanggungjawaban korporasi (*corporate criminal liability*) yang semakin diperkuat dalam perkembangan hukum pidana ekonomi kontemporer.

Selain ketiga bentuk tanggung jawab tersebut, kewajiban pemberitahuan tertulis kepada subjek data dan lembaga pengawas dalam hal terjadi kegagalan perlindungan data pribadi, sebagaimana diatur Pasal 46 UU PDP, menjadi instrumen penting untuk memastikan akuntabilitas penyelenggara *platform* digital. Ketentuan ini mewajibkan pengendali data untuk menyampaikan pemberitahuan tertulis paling lambat tiga kali dua puluh empat jam sejak diketahuinya kegagalan perlindungan data pribadi, yang mencakup data pribadi yang bocor, kapan dan bagaimana data pribadi bocor, serta upaya penanganan dan pemulihan yang telah dilakukan oleh pengendali data. Kewajiban ini secara khusus krusial bagi data biometrik, mengingat sifat permanen dan ireversibelnya menuntut respons cepat agar subjek data dapat segera mengambil langkah mitigasi risiko begitu mengetahui kebocoran data yang menyimpannya.

5. Efektivitas Pengaturan Hukum di Indonesia dan Tantangan Implementasinya

Meskipun kerangka normatif perlindungan data biometrik di Indonesia telah cukup komprehensif pascapengesahan UU PDP, efektivitas implementasinya di lapangan masih menghadapi sejumlah tantangan struktural dan praktis.

Pertama, tantangan kelembagaan. UU PDP mengamanatkan pembentukan lembaga pengawas independen yang berwenang mengawasi kepatuhan pengendali data pribadi, menerima pengaduan, dan menjatuhkan sanksi administratif. Namun, operasionalisasi lembaga tersebut memerlukan waktu, sumber daya manusia yang kompeten di bidang teknologi dan hukum, serta infrastruktur pengawasan yang memadai untuk mampu mengawasi ribuan penyelenggara sistem elektronik yang beroperasi di Indonesia, termasuk *platform* digital lintas batas yang memproses data biometrik penggunaanya dari server yang berlokasi di luar yurisdiksi Indonesia. Keterbatasan kelembagaan ini menyebabkan penegakan hukum terhadap pelanggaran pemrosesan data biometrik cenderung bersifat reaktif, yaitu baru dilakukan setelah muncul pemberitaan publik atau pengaduan, alih-alih bersifat proaktif melalui pengawasan berkala.

Kedua, tantangan kepatuhan penyelenggara sistem elektronik terhadap kewajiban penilaian dampak perlindungan data pribadi. Sebagaimana ditunjukkan dalam kasus *platform* pemindaian iris mata yang beroperasi di Indonesia tanpa DPIA yang memadai, kewajiban ini pada praktiknya kerap diabaikan oleh penyelenggara *platform* digital, terutama yang berbasis di luar negeri dan belum sepenuhnya memahami atau mematuhi rezim hukum perlindungan data pribadi Indonesia. Ketiadaan kewajiban sertifikasi atau audit independen berkala atas sistem yang memproses data biometrik turut memperbesar celah antara norma dan praktik.

Ketiga, tantangan literasi digital masyarakat. Efektivitas mekanisme persetujuan sebagai dasar pemrosesan data biometrik sangat bergantung pada pemahaman substansial pengguna atas risiko yang melekat pada data tersebut. Rendahnya literasi digital menyebabkan banyak pengguna memberikan persetujuan tanpa memahami secara penuh implikasi jangka panjang dari pemberian data biometrik kepada *platform* digital, sehingga esensi “persetujuan yang sah” secara substansial tereduksi menjadi formalitas administratif belaka.

Keempat, tantangan yurisdiksi lintas batas. Banyak *platform* digital yang memanfaatkan data biometrik beroperasi secara global dan menyimpan data penggunaanya di server yang berlokasi di luar Indonesia. Meskipun UU PDP menganut prinsip perlindungan ekstrateritorial yang menjangkau pengendali data di luar wilayah hukum Indonesia sepanjang kegiatan pemrosesan tersebut memiliki akibat hukum bagi subjek data di Indonesia, penegakan hukum terhadap pengendali data yang tidak memiliki kehadiran fisik maupun perwakilan hukum di Indonesia tetap menghadapi kendala praktis yang signifikan, termasuk dalam hal eksekusi sanksi administratif maupun proses penegakan hukum pidana.

Kelima, tantangan harmonisasi sektoral. Pemrosesan data biometrik yang terkait dengan data kesehatan, misalnya dalam konteks verifikasi identitas berbasis kondisi fisiologis tertentu, turut bersinggungan dengan Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan, yang mengatur perlindungan data kesehatan sebagai bagian dari rekam medis elektronik. Ketiadaan harmonisasi yang jelas antara rezim UU PDP dan rezim sektoral kesehatan berpotensi menimbulkan ketidakpastian mengenai regulator yang berwenang dan standar perlindungan yang berlaku ketika data biometrik yang diproses *platform* digital bersinggungan dengan data kesehatan individu.

Berdasarkan pemetaan tantangan tersebut, dapat disimpulkan bahwa efektivitas pengaturan hukum perlindungan data biometrik di Indonesia masih bersifat “efektif secara normatif, namun terbatas secara implementatif”. Kerangka hukum yang ada telah memberikan landasan yang memadai untuk menuntut

pertanggungjawaban penyelenggara *platform* digital, tetapi kapasitas penegakan dan pengawasan yang masih berkembang menyebabkan perlindungan aktual bagi pengguna belum sepenuhnya optimal. Untuk memperkuat efektivitas tersebut, diperlukan langkah-langkah strategis, antara lain percepatan operasionalisasi lembaga pengawas independen dengan kewenangan investigasi dan penegakan yang memadai, penyusunan peraturan turunan yang secara khusus mengatur standar keamanan teknis bagi pemrosesan data biometrik, kewajiban sertifikasi keamanan sistem bagi penyelenggara yang memproses data biometrik dalam skala besar, penguatan kerja sama internasional untuk penegakan hukum lintas yurisdiksi, serta program literasi digital yang menasar pemahaman masyarakat mengenai risiko spesifik data biometrik.

KESIMPULAN

Berdasarkan hasil analisis yang telah diuraikan, dapat disimpulkan tiga hal pokok. Pertama, pengaturan hukum mengenai perlindungan data biometrik di Indonesia telah menempatkannya sebagai data pribadi yang bersifat spesifik sebagaimana diatur Pasal 4 ayat (2) UU PDP, yang merupakan perwujudan konkret dari hak atas privasi yang dijamin Pasal 28G ayat (1) UUD 1945, sehingga menuntut dasar pemrosesan dan standar perlindungan yang lebih ketat dibandingkan data pribadi umum. Kedua, bentuk perlindungan hukum terhadap pengguna terwujud dalam pengaturan mengenai dasar pemrosesan dan persetujuan eksplisit (Pasal 20-21 UU PDP), kewajiban keamanan dan penilaian dampak perlindungan data (Pasal 34-39 UU PDP), hak-hak subjek data (Pasal 5-16 UU PDP), serta tanggung jawab hukum penyelenggara *platform* digital sebagai pengendali data yang bersifat administratif, perdata, dan pidana (Pasal 46, 57, dan 67-73 UU PDP), yang diperkuat oleh ketentuan persetujuan penggunaan data pribadi dalam Pasal 26 UU ITE dan kewajiban keandalan sistem elektronik dalam PP PSTE. Ketiga, efektivitas pengaturan hukum tersebut masih bersifat terbatas secara implementatif, mengingat tantangan kelembagaan pengawas yang belum sepenuhnya operasional, rendahnya kepatuhan penyelenggara *platform* terhadap kewajiban DPIA, minimnya literasi digital masyarakat, kendala yurisdiksi lintas batas, serta kebutuhan harmonisasi dengan regulasi sektoral seperti Undang-Undang Kesehatan. Penelitian ini merekomendasikan percepatan operasionalisasi lembaga pengawas independen, penyusunan regulasi teknis mengenai standar keamanan data biometrik, kewajiban sertifikasi sistem, penguatan kerja sama penegakan hukum lintas yurisdiksi, serta penguatan literasi digital masyarakat. Penelitian lanjutan disarankan untuk mengkaji secara empiris efektivitas penegakan sanksi administratif UU PDP terhadap *platform* digital yang memproses data biometrik, guna memperkuat basis data bagi perumusan kebijakan yang lebih responsif.

DAFTAR PUSTAKA

- Djafar, W., dkk. (2016). *Perlindungan data pribadi di Indonesia: Usulan pelembagaan kebijakan dari perspektif hak asasi manusia*. Lembaga Studi dan Advokasi Masyarakat (ELSAM).
- Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*. Sekretariat Negara.
- Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Sekretariat Negara.
- Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251. Sekretariat Negara.

- Indonesia. (2019). *Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400. Sekretariat Negara.
- Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820. Sekretariat Negara.
- Indonesia. (2023). *Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan*. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 105. Sekretariat Negara.
- Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1. Sekretariat Negara.
- Karo Karo, R. P. P., & Prasetyo. (2020). *Pengaturan perlindungan data pribadi di Indonesia: Perspektif teori keadilan bermartabat*. Nusa Media.
- Kusnadi, S. A., & Wijaya, A. U. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *Jurnal Al-Wasath*, 2(1), 19–32. <https://doi.org/10.47776/alwasath.v2i1.131>
- Marzuki, P. M. (2014). *Penelitian hukum* (Edisi Revisi). Kencana Prenada Media Group.
- Nasakti, G. (2021). Ius constituendum penggunaan teknologi pengenalan wajah dalam industri dan penegakan hukum di Indonesia. *Jurnal Hukum Universitas Pembangunan Nasional "Veteran" Jakarta*, 2(2). <https://repository.upnvj.ac.id/>
- Priliasari, E. (2023). Perlindungan data pribadi konsumen dalam transaksi e-commerce menurut peraturan perundang-undangan di Indonesia. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 12(2), 261–279. <https://doi.org/10.33331/rechtsvinding.v12i2.1121>
- Razaq, M. L. (2023). Penggunaan teknologi pengenalan wajah dalam keamanan publik. *Jurnal Ilmiah Fakultas Hukum Universitas Tarumanagara*, 1(2), 480–487. <https://doi.org/10.24912/jifhum.v1i2.23590>
- Rizki, M. F., & Salam, A. (2023). Pertanggungjawaban hukum pengumpulan data biometrik melalui artificial intelligence tanpa persetujuan pemilik data (Studi kasus Clearview AI Inc. di Yunani dan Inggris). *Lex Patrimonium*, 2(2). <http://dx.doi.org/10.30649/lex.v2i2.128>
- Rosadi, S. D. (2018). *Cyber law: Aspek data privasi menurut hukum internasional, regional, dan nasional*. Refika Aditama.
- Tim Penulis Al-Zayn. (2025). Tanggung jawab hukum platform digital WorldApp atas pemrosesan data biometrik. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(1).
- Tim Penulis Wara Sains. (2023). Pentingnya regulasi khusus tentang pemanfaatan sistem face recognition technology dalam peningkatan keamanan dan penegakan hukum di Indonesia. *Jurnal Hukum dan HAM Wara Sains*, 2(10), 996–1005. <https://doi.org/10.57235/hwarasains.v2i10.1089>