



Perlindungan Data Biometrik Peserta BPJS dalam Implementasi Face Recognition Technology Berdasarkan Undang-Undang Perlindungan Data Pribadi

INFO PENULIS

Rivaldy Archarely Rompis
Universitas Esa Unggul
Rivaldyar98@gmail.com

Annisa Fitria
Universitas Esa Unggul
annisa.fitria@esaunggul.ac.id

INFO ARTIKEL

ISSN: 2808-1307
Vol. 6, No. 2, Agustus 2026
<https://jurnal.ardenjaya.com/index.php/ajsh>

© 2026 Arden Jaya Publisher All rights reserved

Saran Penulisan Referensi

Rompis, R. A., & Fitria, A. (2026). Perlindungan Data Biometrik Peserta BPJS dalam Implementasi Face Recognition Technology Berdasarkan Undang-Undang Perlindungan Data Pribadi. *Arus Jurnal Sosial dan Humaniora*, 6 (2),2494-2500.

Abstrak

Pemanfaatan teknologi Face Recognition pada sistem FRISTA BPJS Kesehatan meningkatkan efisiensi verifikasi peserta Jaminan Kesehatan Nasional (JKN), namun juga menimbulkan tantangan terhadap perlindungan data biometrik. Penelitian ini bertujuan menganalisis penerapan mekanisme persetujuan, transparansi, dan akuntabilitas berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta mengkaji pertanggungjawaban hukum BPJS Kesehatan sebagai pengendali data pribadi. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan konseptual melalui studi kepustakaan yang dianalisis secara deskriptif kualitatif. Hasil penelitian menunjukkan bahwa pemrosesan data biometrik peserta wajib memenuhi prinsip persetujuan eksplisit, transparansi, akuntabilitas, dan keamanan sebagaimana diatur dalam UU PDP. Pertanggungjawaban BPJS Kesehatan berada pada ranah administrasi dan perdata apabila terbukti lalai memenuhi kewajiban perlindungan data, sedangkan pertanggungjawaban pidana pada prinsipnya dibebankan kepada pelaku peretasan sepanjang tidak terdapat keterlibatan pihak internal.

Kata Kunci : Perlindungan Data Pribadi, Data Biometrik, FRT, BPJS Kesehatan, UU PDP

Abstract

The implementation of Face Recognition Technology through BPJS Kesehatan's FRISTA system has enhanced the efficiency of participant verification in Indonesia's National Health Insurance (JKN) program while raising significant concerns regarding biometric data protection. This study aims to analyze the application of consent, transparency, and accountability principles under Law Number 27 of 2022 on Personal Data Protection (PDP Law) and to examine the legal liability of BPJS Kesehatan as the personal data controller in the event of biometric data breaches. This research employs a normative juridical method using statutory and conceptual approaches supported by library research and qualitative descriptive analysis. The findings indicate that biometric data processing must comply with the principles of explicit consent, transparency, accountability, and data security as stipulated in the PDP Law. Nevertheless, implementation remains inadequate due to the absence of implementing Government Regulations governing Face Recognition Technology. BPJS Kesehatan may incur administrative and civil liability for negligence in fulfilling its data protection obligations, while criminal liability primarily rests with external perpetrators unless internal involvement can be established.

Keywords : Personal Data Protection, Biometric Data, FRT, BPJS, PDP Law

A. Pendahuluan

Pemanfaatan teknologi informasi sekarang ini semakin berkembang, terkhususnya perkembangan perlindungan data biometrik di Indonesia yang mengalami kemajuan signifikan yang ditetapkan pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (2022). Aspek keamanan dalam dunia digital menempati posisi utama dalam perlindungan data pribadi, yang mana metode konvensional seperti kata sandi atau kode PIN yang rentan terhadap risiko peretasan dan kelalaian mulai ditinggalkan. Teknologi biometrik merupakan metode identifikasi yang memanfaatkan karakteristik unik individu, misalnya sidik jari, iris mata, suara, dan wajah. Salah satu teknologi biometrik yang paling banyak digunakan adalah Face Recognition Technology (FRT) atau teknologi pengenalan wajah. Teknologi ini telah diterapkan dalam berbagai sektor, baik pemerintahan maupun industri, seperti perbankan dan layanan digital lainnya. Baik digunakan dalam aplikasi pemerintah maupun industri seperti perbankan atau layanan digital lainnya. *Face Recognition Technology* (FRT) merupakan hasil inovasi dari perkembangan teknologi digital di era modern yang mengubah sistem sosial dan hukum dengan mendasar (Husna et al., 2025). Penggunaan data biometrik dalam sistem *Face Recognition* BPJS Kesehatan harus memenuhi prinsip-prinsip pemrosesan data pribadi seperti ditetapkan pada UU PDP, antara lain prinsip persetujuan yang sah, keterbukaan, pembatasan tujuan, akurasi data, keamanan pemrosesan, serta akuntabilitas pengendali data pribadi. Oleh karena itu, implementasi FRISTA perlu dianalisis untuk mengetahui kesesuaiannya dengan ketentuan tersebut.

Fasilitas pelayanan kesehatan merupakan salah satu pilar utama sistem kesehatan nasional, keberhasilan implementasi kebijakan kesehatan nasional yaitu program Jaminan Kesehatan Nasional (JKN) yang dilaksanakan oleh BPJS Kesehatan dilakukan oleh Kementerian Kesehatan Republik Indonesia. Perlindungan data biometrik peserta BPJS Kesehatan, khususnya melalui sistem *Face Recognition* (FRISTA) berbasis AI, telah diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang berlaku efektif secara penuh mulai 17 Oktober 2025. FRT Transformasi Digital dan Kebutuhan Verifikasi Biometrik (FRISTA) BPJS Kesehatan terus melakukan transformasi digital guna meningkatkan layanan Jaminan Kesehatan Nasional (JKN) dan mencapai *Universal Health Coverage*. Sebagai data biometrik, gambar wajah diklasifikasikan menjadi data pribadi yang mempunyai sifat spesifik Pasal 4 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang memerlukan tingkat keamanan lebih tinggi dibandingkan dengan data umum. Dalam implementasinya, sistem FRISTA digunakan terhadap fasilitas kesehatan yang bekerja sama bersama BPJS Kesehatan melalui proses pemindaian wajah peserta untuk memverifikasi identitas secara elektronik. Sistem ini mempergunakan teknologi kecerdasan buatan (*Artificial Intelligence*) yang membandingkan citra wajah peserta dengan data yang tersimpan dalam basis data BPJS Kesehatan guna memastikan kesesuaian identitas dan mencegah penggunaan kartu JKN oleh pihak yang tidak berhak.

Perlindungan tidak hanya menyangkut aspek teknis administrasi, tetapi juga adalah bagian dari HAM yang dijaga oleh negara (Sudrajat, 2020), teknologi ini bertujuan mempermudah layanan, mengurangi antrean di rumah sakit, serta mencegah *fraud* (penyalahgunaan) identitas dalam klaim. Perlindungan data peserta BPJS Kesehatan juga meliputi hak peserta guna memperoleh informasi yang transparan tentang pengelolaan data mereka. Peserta berhak mengetahui mekanisme persetujuan, transparansi, akuntabilitas agar peserta memiliki rasa aman dan kepercayaan bahwa data yang mereka kelola secara bertanggungjawab oleh BPJS Kesehatan. Negara harus memastikan bahwa setiap kebijakan pengelolaan data dilaksanakan dengan prinsip non-diskriminasi dan menghormati hak peserta. Dengan demikian, penguatan regulasi, peningkatan kapasitas pengelolaan data, dan pengawasan yang lebih ketat menjadi langkah penting untuk menghadapi tantangan keamanan data di era digital ini. Akan tetapi, jaminan terhadap perlindungan data pribadi dari sektor pelayanan kesehatan secara digital masih belum terintegrasi dengan baik. Hal ini bisa dibuktikan dengan adanya kasus kebocoran data pribadi kepersertaan Badan Penyelenggara Jaminan Sosial (BPJS) dengan total jumlah 279 juta data pribadi dan informasi mengenai peserta BPJS tersebar dan diperjualkan di Raid Forums (Budiati, 2021). Hal tersebut juga diperkuat dengan adanya statement dari pihak Kementerian Komunikasi yaitu Dedy Permadi yang menyatakan bahwa “Berdasarkan hasil investigasi terhadap sampel data yang terdampak, ditemukan fakta adanya paparan informasi sensitif yang mencakup identitas kartu peserta, detail administratif kantor, riwayat keluarga dan tanggungan asuransi, hingga catatan transaksi iuran.”

Timboel Sitegar selaku Koodinator Bidang Advokasi BPJS Watch menguraikan jika ditemukan terdapatnya dugaan atau akibat dari adanya kebocoran data pada kasus BPJS Kesehatan dikarenakan adanya peretasan aplikasi pihak ketiga dengan diantaranya terdiri dari 8 aplikasi sistem informasi pelayanan kesehatan, 6 aplikasi informasi publik, dan 6 aplikasi pendukung manajemen kepersertaan. Dugaan pertama dikarenakan adanya peretasan, kedua dikarenakan adanya kebocoran data dari pihak internal dan rendahnya tingkat keamanan data pada aplikasi JKN BPJS Kesehatan. Di satu sisi, BPJS Kesehatan mengimplementasikan teknologi Face Recognition sebagai instrumen verifikasi identitas peserta JKN. Namun di sisi lain, belum terdapat pengaturan teknis yang secara khusus mengatur standar pengelolaan, penyimpanan, penghapusan, maupun mekanisme pertanggungjawaban atas data biometrik peserta yang diproses melalui sistem tersebut. Kondisi ini menimbulkan pertanyaan mengenai sejauh mana implementasi *Face Recognition Technology* oleh BPJS Kesehatan telah memenuhi standar perlindungan data pribadi seperti ditetapkan pada UU PDP.

Kasus kebocoran data peserta JKN yang dikelola oleh pihak BPJS Kesehatan mempertegas bahwa data pribadi dari pasien menjadi indikator adanya penyalahgunaan identitas personal dan telah menjadi objek yang rentan disalahgunakan, sehingga perlunya aturan khusus karena hal ini berkaitan dengan hak privasi masyarakat. Berdasarkan penelusuran literatur yang dilakukan, kajian mengenai perlindungan data biometrik peserta BPJS Kesehatan dalam implementasi Face Recognition Technology pasca berlakunya UU PDP masih terbatas, khususnya yang mengkaji penerapan prinsip persetujuan, transparansi, dan akuntabilitas dalam pemrosesan data biometrik. Kebaruan studi yang dilaksanakan terletak pada analisis perlindungan data biometrik peserta BPJS Kesehatan dalam implementasi *Face Recognition Technology* setelah berlakunya UU Nomor 27 Tahun 2022 mengenai Pelindungan Data Pribadi (UU PDP). UU PDP menghadirkan paradigma baru dalam pelindungan data pribadi yang berorientasi pada hak subjek data melalui penerapan prinsip persetujuan yang sah, transparansi, dan akuntabilitas pada pemrosesan data pribadi. Kaitannya dengan konteks penggunaan teknologi pengenalan wajah oleh BPJS Kesehatan, penelitian ini mengkaji sejauh mana pemrosesan data biometrik peserta telah memenuhi prinsip-prinsip tersebut, khususnya terkait pemberian persetujuan, keterbukaan informasi mengenai pengelolaan data, serta tanggung jawab BPJS Kesehatan menjadi kontrol data pribadi dalam menjamin keamanan dan pelindungan data biometrik peserta. Menurut penjelasan tersebut, studi yang dilaksanakan mempunyai tujuan dalam mengidentifikasi perlindungan data biometrik peserta BPJS Kesehatan dalam implementasi Face Recognition Technology berdasarkan UU Nomor 27 Tahun 2022 mengenai Pelindungan Data Pribadi serta menilai kesesuaian penerapannya dengan prinsip-prinsip pelindungan data pribadi. Berdasarkan uraian tersebut, bertujuan bisa memberikan kontribusi bagi pengembangan hukum perlindungan data pribadi di Indonesia, khususnya dalam pemanfaatan teknologi biometrik dalam sektor pelayanan kesehatan.

B. Metodologi

Jenis penelitian yang dipergunakan pada studi yang dilaksanakan yaitu yuridis normatif, penelitian dibentuk melalui studi kepustakaan berdasarkan norma hukum tertulis yang berlaku. Pendekatan perundang-undangan, analisis norma dan asas hukum. Fokus utama adalah kepustakaan (*library research*) yang dianalisis secara kualitatif. Pendekatan Perundang-undangan (*Statute Approach*): Menganalisis konsistensi dan kesesuaian berbagai peraturan perundang-undangan (UU PDP, UU BPJS, UU ITE, serta UU Perlindungan Konsumen) dalam menjamin perlindungan data peserta. Melalui pendekatan ini memberikan ruang bagi penulis untuk mengurai, mendalami, serta mengevaluasi efektivitas aturan hukum dalam memproteksi kerahasiaan data wajah peserta BPJS Kesehatan. Selain itu, cara ini mempermudah proses peninjauan terhadap kapasitas aturan teknis dalam menyediakan panduan operasional yang konkret, guna memastikan adanya perlindungan data pribadi yang konsisten dan memberikan rasa aman bagi seluruh pemegang hak (Efendi et al., 2023).

C. Hasil dan Pembahasan

Bagaimanakah pengaturan mekanisme persetujuan, transparansi, dan akuntabilitas dalam UU PDP terkait perlindungan data biometrik peserta BPJS pada verifikasi Face Recognition AI?

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyebutkan bahwa Presiden memiliki wewenang untuk menetapkan dengan membuat sebuah Peraturan Pemerintah (Asshiddiqie, 2006). Pembentukan PP ini merupakan langkah hukum yang dibutuhkan agar dapat mengimplementasikan amanat dari Pasal 5 ayat 2 UUD RI 1945 yang menyatakan bahwa "*Presiden berwenang menetapkan PP untuk menjalankan undang-undang sebagaimana mestinya*" (Asshiddiqie, 2006). Pembentukan aturan yang mengatur tentang teknologi *Facial Recognition* (FRT) harus disusun secara praktis agar tidak terjadi kekosongan hukum dalam implementasinya. Tahap awal dimulai dengan penetapan landasan hukum yang kuat sebagai kedudukan hukum dari penggunaan teknologi, kemudian diikuti dengan kodifikasi kewajiban ketat bagi pengendali data untuk menjamin keamanan informasi biometrik yang bersifat sensitif dan tak tergantikan. Selain itu, pembentukan aturan tersebut wajib melembagakan mekanisme pengawasan independen dan standar akuntabilitas yang transparan guna memitigasi risiko penyalahgunaan wewenang atau kebocoran data. Sebagai pilar terakhir, aturan ini harus memberikan kepastian hukum melalui prosedur litigasi dan pemulihan hak yang jelas, sehingga masyarakat memiliki saluran resmi untuk menuntut pertanggungjawaban apabila terjadi pelanggaran privasi atau kegagalan sistem yang merugikan.

Penggunaan FRT yang ditetapkan dalam PP menjadi penting dikarenakan dapat mengisi kekosongan hukum dan memberikan kepastian hukum sekaligus bagi negara dan masyarakat terkait penggunaan teknologi ini. Sejalan dengan teori dari Roscoe Pound mengenai *law as a tool of social engineering*, aturan hukum idealnya dioperasikan menjadi perangkat rekayasa sosial guna mengarahkan dinamika masyarakat menuju tatanan yang lebih teratur, berkeadilan, serta menjunjung tinggi nilai-nilai kemanusiaan. Sehingga, PP FRT tidak hanya diposisikan sebagai pedoman teknis semata, melainkan PP FRT juga berfungsi sebagai instrumen penunjang tata kelola dari UU PDP yang memegang peran fundamental yang ditujukan dalam memitigasi risiko pelanggaran hak-hak privat, sekaligus mengoptimalkan nilai guna teknologi melalui prinsip pertanggungjawaban yang ketat (Purwaningtyas et al., 2023). Selain itu, implementasi aturan hukum tersebut wajib mengadopsi prinsip-prinsip perlindungan data internasional yang pada ketetapanannya diimplementasikan pada aspek proporsionalitas, transparansi, serta keterlibatan publik secara aktif. Upaya ini dilakukan agar jaminan keamanan data tidak hanya bersifat prosedural secara formal, melainkan juga mampu menumbuhkan legitimasi dan rasa percaya masyarakat terhadap penggunaan sistem biometrik dalam ekosistem digital yang terus berevolusi. Dengan landasan kedudukan hukum yang kokoh, potensi penyalahgunaan wewenang dalam pengelolaan teknologi FRT dapat diminimalisir demi menjaga kedaulatan data pribadi setiap individu (Prasetyo & Lestari, 2021).

Melalui UU Perlindungan Data Pribadi (UU PDP), pemerintah memberikan payung hukum terhadap informasi yang bersifat unik dan melekat pada individu. Data biometrik, seperti rekaman sidik jari dan struktur wajah, masuk dalam kategori data pribadi spesifik. Hal ini dikarenakan sifatnya yang tidak tergantikan dan menjadi pembeda utama antar individu, sehingga penggunaannya diatur secara ketat guna mencegah penyalahgunaan identitas. Karena tergolong data sensitif, perlakuan terhadap data biometrik harus dilakukan dengan pengamanan yang lebih ketat. UU PDP melalui Pasal 20 ayat (2) menegaskan bahwa pengendali data dilarang mengolah data biometrik dengan tidak terdapatnya persetujuan yang dinyatakan dengan jelas (eksplisit) oleh subjek data yang bersangkutan.

Sementara Pasal 21 mengatur bahwa subjek data yang diolah atau dilakukan pemrosesan harus diberi informasi lengkap mengenai:

1. Legalitas;
2. Tujuan;
3. Jenis dan relevansi atau keakuratan data yang diproses;
4. Jangka waktu retensi dokumen;
5. Rincian informasi;
6. Jangka waktu pengolahan data dan Hak Subjek Data Pribadi.

Oleh karena data biometrik bersifat permanen dan tidak dapat diubah, pengamanannya harus jauh lebih berlapis dibandingkan jenis data lainnya. Di tengah maraknya risiko eksploitasi dan pencurian identitas, UU PDP berperan sebagai instrumen hukum yang krusial untuk memastikan pengelolaan data dilakukan secara terbuka dan sesuai izin. Ketentuan yang termaktub dalam Pasal 20 dan 21 UU PDP memberikan jaminan bahwa individu memiliki

kendali penuh atas maksud dan lamanya data mereka digunakan. Meskipun hal tersebut terbilang seperti memberikan jaminan, efektivitas dari aturan hukum yang dibuat ini harus dibarengi dengan komitmen moral dari pihak perusahaan serta kesadaran publik. Peningkatan literasi digital masyarakat menjadi sangat penting agar setiap orang tidak mudah menyerahkan identitas biologis mereka hanya karena tergiur imbalan sesaat (SIP Law Firm, 2025).

Bagaimana pertanggungjawaban hukum BPJS Kesehatan sebagai pengendali data pribadi apabila terjadi pelanggaran data biometrik akibat penggunaan *Face Recognition AI* menurut UU PDP?

Terkait dengan pertanggungjawaban hukum kesehatan sebagai pengendali data pribadi, apabila dikaitkan dengan konsep perlindungan data pribadi, maka pada dasarnya setiap pengguna atau peserta jkn memiliki hak untuk menentukan apakah dirinya akan melaksanakan *sharing* data ataupun tidak serta hal tersebut sudah seharusnya di paparkan didalam aplikasi tersebut didalam perjanjian atau prasyarat sebelum pemakaian Pemerintah mempunyai peran yang sangat besar untuk menjaga, pengawas serta memperkuat pengelolaan data pribadi di sektor Kesehatan. Penegakan hukum yang konsisten serta tegas pada pelaku kebocoran harus menjadi prioritas utama agar dapat memberikan efek jera yang nyata (Najwa, 2024). Kemajuan teknologi yang semakin maju banyak data yang secara elektronik, potensi terjadi kebocoran data pribadi. Kebocoran data pribadi ini menjadi ancaman yang serius karena tidak hanya rugi secara pribadi tetapi juga menimbulkan dampak social dan ekonomi yang luas bagi masyarakat serta merusak kepercayaan public terhadap program Jaminan Kesehatan Nasional (JKN).

Maka dari itu harus ada pertanggungjawaban hukum terhadap BPJS Kesehatan sebagai pengendali data pribadi apabila terjadi pelanggaran data biometrik akibat penggunaan *Face Recognition AI* menurut UU PDP. Salah satunya dengan adanya sertifikat ISO yang khusus berkaitan dengan keamanan siber, standar internasional, dengan standar ini risiko kebocoran data akibat serangan hacker dapat diminimalkan secara signifikan, sehingga perlindungan terhadap data peserta bisa lebih optimal (Matheus, J., & Gunadi, 2024). Kementerian Kesehatan juga berkolaborasi bersama Dinas Kependudukan dan Catatan Sipil (Dukcapil) dalam menjaga keamanan dan validasi data peserta.

Undang-Undang Nomor 27 Tahun 2022 mengenai perlindunganData Pribadi (UU PDP) mengatur tanggung jawab hukum BPJS Kesehatan sebagai pengendali data pribadi jika terjadi pelanggaran data biometrik akibat penggunaan *Face Recognition AI*. UU DPD bahwa BPJS Kesehatan menjadi pengendali data yang mempunyai nilai perlindungan, mutlak untuk memberikan rasa aman pada saat peserta secara pribadi melakukan proses administratif seperti riwayat kesehatan dan informasi keuangan peserta (Watkat et al., 2024).

Sesuai aturan hukum UU PDP, pertanggungjawaban hukum terbagi menjadi tiga ranah, yaitu secara administrasi, perdata, dan pidana. Berikut adalah ringkasan mengenai posisi BPJS Kesehatan dalam kasus kebocoran data:

1. Pertanggungjawaban Administrasi dan Perdata yaitu BPJS Kesehatan dapat dikenai sanksi administrasi menurut Pasal 57 UU PDP, mulai dari teguran tertulis hingga denda administratif, karena dinilai lalai dalam menjalankan kewajiban perlindungan data.
2. Di sisi lain, sesuai Pasal 12 UU PDP, BPJS Kesehatan juga dapat dituntut secara perdata melalui gugatan wanprestasi atau Perbuatan Melawan Hukum (PMH) jika pemilik data mengalami kerugian akibat kebocoran tersebut.
3. Pertanggungjawaban Pidana yaitu apabila dikaji Secara hukum pidana, BPJS Kesehatan tidak dapat dimintai pertanggungjawaban atas insiden tersebut. Hal ini dikarenakan kebocoran data dipicu oleh tindakan pihak luar atau peretas, bukan dilakukan oleh instansi itu sendiri. Meskipun proses pemeriksaan forensik digital masih berjalan, fokus tuntutan pidana tetap tertuju pada pelaku penyerangan sistem.

BPJS Kesehatan adalah badan hukum pemerintah yang memiliki fungsi pelayanan publik mempergunakan tata cara yang ditetapkan sedemikian rupa guna memudahkan asyarakat dalam mengakses layanan kesehatan pada skema jaminan sosial. Status ini tidak meniadakan pertanggungjawaban perdata Ketika terjadi kerugian pada peserta akibat pelanggaran hak-hak privat, termasuk hak atas perlindungan data pribadi. Secara doktrinal, tanggung gugat perdata lazim dibangun melalui dua jalur, yakni wanprestasi (jika terdapat hubungan perikatan yang dilanggar) atau PMH (jika kerugian timbul dari pelanggaran kewajiban hukum umum) (Subekti, 2008). Dalam konteks kebocoran data, hubungan peserta BPJS lebih tepat diposisikan sebagai PMH karena kewajiban melindungi data dan memberi notifikasi kegagalan perlindungan terutama bersumber dari peraturan perundang-undangan dan prinsip kehati-hatian pengelola sistem elektronik. PMH menurut Pasal 1365 KUH Perdata memberikan persyaratan terdapatnya Tindakan melawan hukum, kesalahan, kerugian, serta hubungan kausal antara tindakan dan

kerugian. Doktrin juga mengakui bahwa perbuatan dapat berupa tindakan aktif maupun kelalaian (*omission*) ketika pelaku memiliki kewajiban hukum untuk bertindak. Dalam perkara kebocoran data, perbuatan melawan hukum dapat berbentuk:

1. Kegagalan menerapkan standar keamanan yang wajar sehingga membuka celah kebocoran;
2. Kegagalan melakukan pemberitahuan kepada subjek data sebagaimana diperintahkan peraturan; dan/atau
3. Kegagalan melakukan langkah pemulihan yang patut ketika insiden diketahui.

Penting untuk dipahami bahwa dalam setiap kebocoran data, yang menjadi korban bukan sekadar angka atau deretan kode, melainkan privasi jutaan individu. Narasi hukum yang berkembang saat itu menegaskan bahwa fokus pertanggungjawaban tidak boleh hanya berhenti pada pengejaran peretas sebagai aktor kriminal, tetapi harus menyentuh sisi manajerial: sejauh mana pengelola data telah menjalankan prinsip kehati-hatian dalam menjaga amanah data tersebut. Pada akhirnya, pertanggungjawaban hukum BPJS Kesehatan bukan hanya soal membayar denda atau memenangkan gugatan di pengadilan. Ini adalah tentang membangun kembali kontrak sosial dan kepercayaan digital antara warga negara dengan pengelolanya. UU PDP telah memberikan fondasi yang kuat, namun efektivitasnya akan sangat bergantung pada konsistensi penegakan hukum, transparansi institusi, dan kesadaran kolektif akan pentingnya melindungi kedaulatan data pribadi di era digital.

D. Kesimpulan

Data biometrik berupa citra wajah peserta BPJS merupakan data pribadi yang bersifat spesifik sehingga pemrosesannya wajib memenuhi prinsip persetujuan eksplisit, transparansi, akuntabilitas, serta keamanan sebagaimana diatur dalam UU PDP. Namun, implementasi perlindungan tersebut belum optimal karena belum adanya Peraturan Pemerintah yang mengatur secara teknis penggunaan *Face Recognition Technology* sehingga masih terdapat kelemahan dalam pengawasan dan kepastian hukum.

Pertanggungjawaban hukum BPJS Kesehatan atas pelanggaran data biometrik dalam penggunaan *Face Recognition AI* menurut UU PDP berada pada ranah administrasi dan perdata apabila terbukti lalai memenuhi kewajiban sebagai Pengendali Data Pribadi, seperti menjaga keamanan sistem, melakukan pemberitahuan kepada subjek data, dan melaksanakan langkah pemulihan sebagaimana diatur dalam UU PDP. Adapun dalam ranah pidana, BPJS Kesehatan tidak serta-merta dapat dimintai pertanggungjawaban karena kebocoran data disebabkan oleh tindakan pihak luar berupa peretasan. Meskipun proses pemeriksaan forensik digital dilakukan untuk mengidentifikasi penyebab serta pelaku kebocoran data, fokus pertanggungjawaban pidana tetap diarahkan kepada pelaku peretasan sepanjang tidak ditemukan bukti adanya kesengajaan atau keterlibatan pihak internal BPJS dalam tindak pidana tersebut. Pertanggungjawaban hukum BPJS Kesehatan sebagai Pengendali Data Pribadi pada prinsipnya lebih menitikberatkan pada tanggung jawab administrasi dan perdata apabila terjadi kelalaian dalam pemenuhan kewajiban perlindungan data. Sementara itu, pertanggungjawaban pidana lebih diarahkan kepada pelaku yang secara melawan hukum melakukan akses, pengambilan, atau penyebaran data pribadi, kecuali dapat dibuktikan adanya keterlibatan pihak internal BPJS dalam tindak pidana tersebut.

E. Refrensi

- Asshiddiqie, J. (2006). *Perihal Undang-Undang*. Jakarta: Konstitusi Press.
- Authme. (2024). *Mengenal Face Recognition: Pengertian, Cara Kerja, Manfaat dan Aplikasinya dalam Verifikasi Identitas*. Authme. Diakses pada 26 April 2026 pukul 12:47 dari tautan: <https://authme.com/id/blog/understanding-face-recognition/>
- Budhijanto, D. (2023). *Hukum Pelindungan Data Pribadi di Indonesia: Cyberlaw & Cybersecurity*. Bandung: Refika Aditama.
- Budiati, A. D. (2021). *Dua Dugaan Penyebab Kebocoran 279 Juta Data Pribadi Diklaim Peserta BPJS*. dream.co.id. Diakses pada 28 April 2026 pukul 08:00 dari tautan: <https://www.dream.co.id/dinar/2-hal-ini-diduga-jadi-biang-kerok-kebocoran-data-penduduk-210524f.html>
- CNN Indonesia. (2021). *Kebocoran Data Pribadi, BPJS Kesehatan Bakal Digugat*. CNN Indonesia. Diakses pada 26 April 2026 pukul 07:50 dari tautan: <https://www.cnnindonesia.com/teknologi/20210606200515-185-650991/kebocoran-data-pribadi-bpjs-kesehatan-bakal-digugat>

- Dewi, S. (2017). Prinsip – Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional dan Implementasinya. *Sosiohumaniora*, 19(3), 206 – 212.
- Efendi, A., Susanti, D. O., & Tektona, R. I. (2023). *Penelitian Hukum Doktrinal*. Yogyakarta: LaksBang Justitia.
- Fanny, P. (2019). Perlindungan Privasi data Pribadi Perspektif Perbandingan Hukum. *Jatiswara*, 34(3), 239–249.
- Husna, N., Nurman, M., & Nugroho, Y. (2025). Pembentukan Peraturan Pemerintah Tentang Face Recognition Technology Ditinjau dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Jurnal Ilmiah AKSES*, 3(2), 1–6.
- Kitab Undang-Undang Hukum Perdata (KUHPerdata).
- Matheus, J., & Gunadi, A. (2024). Pembentukan lembaga pengawas perlindungan data pribadi di era ekonomi digital: Kajian perbandingan dengan KPPU. *Justisi*, 10(1), 20–35.
- Najwa, F. R. (2024). Analisis hukum terhadap tantangan keamanan siber: Studi kasus penegakan hukum siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum*, 2(1), 8–16.
- Prasetyo, T. A., & Lestari, I. A. (2021). Regulasi dan Tantangan Teknologi Face Recognition di Indonesia. *Jurnal Hukum dan Teknologi*, 5(2), 75–90.
- Purwaningtyas, L. A., Anggono, B. D., & Efendi, A. (2023). Pendelegasian Wewenang Pembentukan Undang-Undang oleh Undang-Undang. *Interdisciplinary Journal On Law, Social Sciences And Humanities*, 4(1), 21.
- Rivantoro, R., & Asri, D. P. B. (2026). Tanggung Jawab Hukum Korporasi Atas Kebocoran Data Peserta BPJS Kesehatan Berdasarkan UU No. 27 Tahun 2022. *Jurnal Pengabdian Masyarakat dan Riset Pendidikan*, 4(3), 16034–16040.
- Rosadi, S. (2025). *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*. Jakarta: Refika Aditama.
- SIP Law Firm. (2025). *Antara Inovasi dan Ancaman Privasi, Ini Urgensi Perlindungan Data Biometrik di Era AI*. SIP Law Firm. Diakses pada 28 April 2026 pukul 08:19 dari tautan: <https://siplawfirm.id/perindungan-data-biometrik?lang=id>
- Subekti, R. (2008). *Hukum Perjanjian*. Jakarta: Intermasa.
- Sudrajat, T. (2020). Perlindungan Hukum dan Pemenuhan Hak Pekerja pada Program Jaminan Kesehatan Nasional. *Pandecta Research Law Journal*, 15(1), 83–92.
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (1945).
- Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (2016).
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (2022).
- Undang – Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (1999).
- Watkot, F. X., Ingratubun, M. T., Ingsaputro, M. H., & Hartantyo, A. T. (2024). Pertanggungjawaban pidana pengendali data pribadi terhadap kebocoran data pribadi warga negara Indonesia. *Jurnal Hukum Ius Publicum*, 5(2), 177–198.
- Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi Di Indonesia. *Jurnal Becoss*, 1(1), 147–154.