

PERLINDUNGAN HUKUM TERHADAP PENYALAHGUNAAN DATA BIOMETRIK DALAM PERSPEKTIF UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI

Cheny Berlian, Abdul Aziz

Fakultas Hukum, Universitas Muhammadiyah Riau

chenyberlian@umri.ac.id, abdulaziz@umri.ac.id

Abstrak

Transformasi teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah menginisiasi penggunaan informasi pribadi yang bersifat biometrik di berbagai sektor kehidupan, seperti perbankan, layanan keuangan digital, telekomunikasi, kesehatan, dan pelayanan publik. Data biometrik berupa sidik jari, wajah, retina mata, suara, maupun karakteristik biologis lainnya memiliki karakteristik biologis yang bersifat permanen dan mampu mengidentifikasi seseorang secara individual sehingga penggunaannya semakin luas sebagai sarana identifikasi dan autentikasi. Di sisi lain, penggunaan data biometrik menimbulkan risiko hukum apabila terjadi penyalahgunaan, kebocoran, atau pemrosesan tanpa persetujuan pemilik data. Berbeda dengan kata sandi atau identitas digital lainnya, data biometrik tidak dapat dengan mudah diganti ketika mengalami kebocoran sehingga berpotensi menimbulkan kerugian yang lebih besar bagi pemilik data. Kajian ini difokuskan pada telaah terhadap pengaturan hukum yang mengatur perlindungan data biometrik sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan mengkaji bentuk perlindungan hukum terhadap penyalahgunaan data biometrik. Kajian ini disusun dengan menggunakan penelitian hukum normatif yang menerapkan pendekatan peraturan perundang-undangan (*statute approach*) untuk mengkaji ketentuan hukum yang mengatur perlindungan data biometrik di Indonesia dan juga pendekatan konseptual. Berdasarkan hasil analisis diketahui bahwa data biometrik dikategorikan sebagai data pribadi yang bersifat spesifik sehingga memperoleh perlindungan hukum yang lebih ketat dibandingkan data pribadi umum. Perlindungan hukum dilakukan melalui mekanisme preventif dan represif yang meliputi hak subjek data, kewajiban pengendali data, sanksi administratif, serta sanksi pidana. Namun demikian, efektivitas perlindungan hukum masih menghadapi kendala berupa keterbatasan regulasi teknis, lemahnya pengawasan, dan rendahnya kesadaran masyarakat mengenai pentingnya perlindungan data pribadi.

Kata Kunci: Data Biometrik, Perlindungan Hukum, Data Pribadi, UU PDP, Kejahatan Siber.

Abstract

The transformation of information and communication technology in recent decades has fueled the use of biometric personal information in various sectors of life, such as banking, digital financial services, telecommunications, healthcare, and public services. Biometric data, in the form of fingerprints, facial features, retinal features, voice features, and other biological characteristics, is permanent and capable of individually identifying individuals, increasing its use as a means of identification and authentication. On the other hand, the use of biometric data poses legal risks in the event of misuse, leakage, or processing without the data owner's consent. Unlike passwords or other digital identities, biometric data cannot be easily replaced in the event of a breach, potentially resulting in greater losses for data owners. This study focuses on examining the legal provisions governing biometric data protection as stipulated in Law Number 27 of 2022 concerning Personal Data Protection and examines the forms of legal protection against biometric data misuse. This study is conducted using normative legal research, applying a statutory approach to examining the legal provisions governing biometric data protection in Indonesia, as well as a conceptual approach. This analysis reveals that biometric data is categorized as specific personal data and therefore receives stricter legal protection than general personal data. Legal protection is implemented through

prevention and enforcement mechanisms, which encompass data subject rights, data controller obligations, administrative sanctions, and criminal sanctions. However, the effectiveness of legal protection still faces challenges in the form of limited technical regulations, weak oversight, and low public awareness of the importance of personal data protection.

Keywords: *Biometric Data, Legal Protection, Personal Data, PDP Law, Cybercrime.*

PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi telah membawa perubahan yang signifikan terhadap berbagai aspek kehidupan, mulai dari kehidupan masyarakat, pemerintahan, pendidikan, kesehatan, perbankan, hingga perdagangan elektronik. Transformasi digital tersebut menghasilkan peningkatan pengumpulan, pengolahan, penyimpanan, dan distribusi data pribadi masyarakat dalam jumlah yang sangat besar. Dewasa ini data yang bersifat pribadi telah menjadi salah satu aset yang memiliki nilai ekonomi tinggi sekaligus menjadi objek yang rentan terhadap berbagai bentuk kejahatan siber. Dalam konteks ini, perlindungan data pribadi menjadi isu hukum yang semakin penting karena berkaitan erat dengan hak privasi, keamanan individu, dan perlindungan hak asasi manusia.

Hak privasi terhadap data pribadi merupakan salah satu hak mendasar yang berperan penting dalam melindungi martabat manusia dan menjadi landasan bagi berbagai hak asasi manusia lainnya. Menurut Danrivanto Budhijanto (Wibowo, 2025), hak privasi sebagai bagian dari hak asasi manusia mencakup perlindungan terhadap hak-hak pribadi atau privat. Perlindungan ini memiliki banyak manfaat, seperti memperkuat nilai-nilai kemanusiaan, mempererat hubungan antara individu dan masyarakat, meningkatkan otonomi pribadi untuk mengontrol dan menentukan kepentingan, serta mendorong toleransi dan menghindari diskriminasi. Selain itu, perlindungan hak privasi juga berfungsi untuk membatasi penyalahgunaan kekuasaan oleh pemerintah.

Keberadaan data pribadi memiliki fungsi yang sangat penting dalam sistem layanan elektronik karena menjadi dasar untuk mengidentifikasi setiap pengguna. Informasi tersebut dapat berupa identitas kependudukan, data kontak, maupun informasi lain yang berkaitan dengan seseorang. Di Indonesia, data kependudukan yang tercantum dalam Kartu Tanda Penduduk (KTP) masih menjadi bentuk identitas yang paling sering dimanfaatkan dalam berbagai pelayanan administrasi dan transaksi. Seiring meningkatnya penggunaan layanan berbasis digital, pemrosesan data pribadi juga menjadi bagian yang tidak terpisahkan dari registrasi aplikasi, layanan perbankan digital, klaim asuransi, fasilitas *buy now pay later* (BNPL), hingga berbagai layanan elektronik lainnya.

Dalam penyelenggaraan sistem elektronik, data pribadi berfungsi sebagai identitas yang memungkinkan seseorang dikenali secara individual. Informasi tersebut tidak hanya mencakup identitas kependudukan, nama, alamat, nomor telepon, dan alamat surat elektronik, tetapi juga meliputi informasi keuangan, rekam medis, data genetik, serta data biometrik yang memiliki tingkat sensitivitas lebih tinggi. Mengingat data-data tersebut berkaitan erat dengan hak privasi seseorang, setiap bentuk pengumpulan, penyimpanan, penggunaan, maupun pengungkapannya harus dilakukan sesuai dengan ketentuan hukum yang berlaku agar terhindar dari penyalahgunaan.

Data-data terkait data pribadi dapat dijabarkan dengan perluasan berdasarkan UU PDP, yaitu sebagai berikut ini:

Tabel 1.

Klasifikasi Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Kategori Data Pribadi	Uraian	Contoh
Data Pribadi yang Bersifat Umum	Data pribadi yang berkaitan dengan identitas seseorang dan dapat digunakan untuk mengenali atau mengidentifikasi individu,	1. Nama lengkap 2. Jenis kelamin 3. Kewarganegaraan 4. Agama 5. Status perkawinan

	baik secara langsung maupun tidak langsung.	6. Data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.
Data Pribadi yang Bersifat Spesifik	Data pribadi yang memiliki tingkat sensitivitas lebih tinggi sehingga memerlukan perlindungan hukum khusus karena berpotensi menimbulkan kerugian yang lebih besar apabila disalahgunakan.	1. Data dan informasi kesehatan 2. Data biometrik 3. Data genetika 4. Catatan kejahatan 5. Data anak 6. Data keuangan pribadi 7. Data lainnya sesuai ketentuan peraturan perundang-undangan.

Sumber: Diolah oleh penulis berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Banyaknya kasus-kasus kebocoran data pribadi yang terjadi menunjukkan bahwa hak privasi warga negara Indonesia sangat riskan terhadap penyalahgunaan (Teddy Lesmana, 2022) yang mana dapat menyebabkan kerugian bagi banyak kalangan. Pelanggaran terhadap data pribadi tidak hanya disebabkan oleh kebocoran data semata, tetapi juga oleh pengolahan data pribadi yang dilakukan secara tidak bertanggung jawab.

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan mendasar dalam berbagai aspek kehidupan masyarakat. Digitalisasi yang semakin masif menyebabkan meningkatnya penggunaan data pribadi dalam berbagai aktivitas elektronik, mulai dari transaksi keuangan, pelayanan publik, pendidikan, kesehatan, hingga aktivitas perdagangan elektronik. Salah satu jenis data pribadi yang semakin banyak digunakan adalah data biometrik yang berfungsi sebagai sarana identifikasi dan autentikasi individu dalam sistem digital.

Data biometrik merupakan data yang berkaitan dengan karakteristik fisik, fisiologis, maupun perilaku seseorang yang memungkinkan identifikasi unik terhadap individu tertentu. Bentuk data biometrik meliputi sidik jari, pengenalan wajah (*face recognition*), retina mata, iris mata, DNA, serta karakteristik biologis lainnya. Dalam praktiknya, penggunaan data biometrik dinilai lebih aman dibandingkan penggunaan kata sandi konvensional karena memiliki tingkat keunikan yang tinggi dan sulit dipalsukan. Namun, penggunaan data biometrik juga menghadirkan berbagai risiko hukum, terutama apabila terjadi penyalahgunaan atau kebocoran data.

Melansir data World Bank Group (Group, 2018), data biometrik terdiri dari beberapa jenis. Berikut data biometrik yang sering digunakan dalam teknologi keamanan:

Tabel 2.
Jenis Data Biometrik berdasarkan World Bank Group

Kategori	Jenis Data Biometrik	Keterangan
Biologis	Sidik Jari (<i>Fingerprints</i>)	Pola unik pada ujung jari yang umum digunakan untuk <i>autentikasi digital</i> .
Biologis	Wajah (<i>Face</i>)	Karakteristik wajah seperti struktur tulang, jarak mata, dan bentuk hidung untuk pengenalan wajah.
Biologis	Iris (<i>Iris Scans</i>)	Pola unik pada iris mata dengan tingkat akurasi identifikasi yang tinggi.

Biologis	Pola Pembuluh Darah (<i>Veins</i>)	Pola vena pada tangan atau wajah yang dimanfaatkan dalam teknologi biometrik.
Perilaku	Dinamika Ketikan (<i>Keystroke Dynamics</i>)	Pola pengetikan berdasarkan kecepatan, ritme, dan interval penekanan tombol.
Perilaku	Gaya Berjalan (<i>Gait</i>)	Karakteristik cara berjalan yang dapat digunakan untuk identifikasi individu.
Perilaku	Tanda Tangan (<i>Signature</i>)	Karakteristik tanda tangan, termasuk tekanan dan kecepatan saat menulis.
Perilaku	Suara (<i>Voice</i>)	Karakteristik suara, seperti nada dan frekuensi, untuk pengenalan identitas.

Sumber: Diolah oleh penulis berdasarkan World Bank Group.

Urgensi perlindungan terhadap data biometrik semakin meningkat seiring berkembangnya teknologi kecerdasan buatan (*Artificial Intelligence*), sistem pengenalan wajah, serta berbagai layanan digital yang memanfaatkan identitas biometrik sebagai alat verifikasi. Berbeda dengan kata sandi yang dapat diganti apabila mengalami kebocoran, data biometrik bersifat permanen dan melekat pada individu sehingga kebocoran data biometrik dapat menimbulkan dampak jangka panjang terhadap privasi dan keamanan pemilik data. Risiko tersebut meliputi pencurian identitas, pemalsuan identitas digital, penyalahgunaan akun elektronik, hingga pelanggaran hak privasi.

Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Undang-undang tersebut mengatur berbagai aspek perlindungan data pribadi, mulai dari hak subjek data, kewajiban pengendali data, mekanisme pemrosesan data, hingga sanksi administratif dan pidana terhadap pelanggaran data pribadi. Pasal 4 UU PDP secara tegas menyatakan bahwa data biometrik termasuk kategori data pribadi yang bersifat spesifik sehingga memerlukan perlindungan hukum yang lebih ketat karena berpotensi menimbulkan dampak yang lebih besar terhadap subjek data apabila terjadi penyalahgunaan.

Meskipun demikian, keberadaan UU PDP belum sepenuhnya menjamin terlaksananya perlindungan data biometrik secara optimal. Masih terdapat berbagai tantangan dalam implementasinya, antara lain belum lengkapnya regulasi teknis, keterbatasan pengawasan, serta meningkatnya penggunaan teknologi berbasis biometrik oleh berbagai sektor tanpa diimbangi dengan mekanisme perlindungan yang memadai. Kondisi tersebut menunjukkan perlunya kajian lebih lanjut mengenai bentuk perlindungan hukum terhadap penyalahgunaan data biometrik dalam sistem hukum Indonesia.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif yang berorientasi pada kajian terhadap norma-norma hukum yang berlaku sebagai dasar dalam menganalisis permasalahan hukum (Sidharta, 2013). Penelitian ini bersifat deskriptif-analitis karena bertujuan untuk memberikan gambaran secara sistematis mengenai pengaturan perlindungan hukum terhadap penyalahgunaan data biometrik berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, sekaligus menganalisis berbagai persoalan hukum yang muncul dalam penerapannya.

Bahan hukum yang digunakan terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan perlindungan data pribadi, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang

Pelindungan Data Pribadi. Sementara itu, bahan hukum sekunder diperoleh dari buku-buku ilmiah, artikel jurnal, hasil penelitian, serta literatur lain yang relevan dengan objek penelitian. Selain itu, penulis juga memanfaatkan sumber elektronik yang memiliki kredibilitas untuk memperkaya analisis terhadap isu yang dikaji.

Penelitian ini menggunakan pendekatan yuridis normatif atau doctrinal legal research, yaitu penelitian yang menitikberatkan kajian pada norma hukum yang terdapat dalam peraturan perundang-undangan, doktrin, putusan pengadilan, serta pendapat para ahli hukum. Seluruh bahan hukum yang telah dikumpulkan kemudian dianalisis secara kualitatif melalui penafsiran terhadap norma hukum sehingga diperoleh argumentasi hukum yang mampu menjawab rumusan masalah penelitian (Waluyo, 1991).

Dalam pelaksanaannya, penelitian hukum normatif lebih menekankan studi kepustakaan (library research) sebagai sumber utama pengumpulan bahan hukum. Untuk memperoleh analisis yang komprehensif, penelitian ini menggunakan pendekatan perundang-undangan (statute approach) guna mengkaji ketentuan hukum yang berlaku serta pendekatan konseptual (conceptual approach) untuk menelaah berbagai konsep dan doktrin hukum yang berkaitan dengan perlindungan data biometrik. Pendekatan tersebut dipilih karena dinilai paling relevan dalam menjelaskan permasalahan hukum yang menjadi fokus penelitian (Soekanto & Mamudji, 2001).

HASIL DAN PEMBAHASAN

Pengaturan Perlindungan Hukum terhadap Data Biometrik dalam UU PDP

Ketentuan mengenai kewajiban menjaga keamanan data pribadi diatur dalam Pasal 35 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Ketentuan tersebut mewajibkan setiap Pengendali Data Pribadi untuk menerapkan sistem perlindungan yang mampu menjamin keamanan data selama proses pengumpulan, penyimpanan, penggunaan, hingga pemusnahannya. Upaya tersebut diwujudkan melalui penerapan langkah-langkah teknis dan operasional yang disesuaikan dengan karakteristik data serta tingkat risiko yang mungkin timbul akibat pemrosesan data pribadi. Dengan demikian, setiap proses pengelolaan data harus dirancang sedemikian rupa agar terhindar dari akses tanpa hak, penyalahgunaan, maupun bentuk pemrosesan lain yang bertentangan dengan ketentuan peraturan perundang-undangan (Kurniawan Tri Wibowo, 2025).

Tabel 3.

Bentuk penyalahgunaan data biometrik dan ancaman pidana menurut UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Bentuk Penyalahgunaan Data Biometrik	Ketentuan UU PDP	Ancaman Pidana
Mengambil data biometrik tanpa izin	Pasal 65 ayat (1) jo. Pasal 67 ayat (1)	Penjara paling lama 5 tahun dan/atau denda paling banyak Rp5 miliar.
Membocorkan data biometrik kepada pihak lain	Pasal 65 ayat (2) jo. Pasal 67 ayat (2)	Penjara paling lama 4 tahun dan/atau denda paling banyak Rp4 miliar.
Menggunakan data biometrik tanpa hak	Pasal 65 ayat (3) jo. Pasal 67 ayat (3)	Penjara paling lama 5 tahun dan/atau denda paling banyak Rp5 miliar.
Memalsukan identitas biometrik atau data pribadi	Pasal 66 jo. Pasal 68	Penjara paling lama 6 tahun dan/atau denda paling banyak Rp6 miliar.

Sumber: Diolah oleh penulis berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Pengaturan mengenai data biometrik di Indonesia memperoleh landasan hukum yang kuat setelah disahkannya UU PDP. Dalam Pasal 4 ayat (2), data biometrik diklasifikasikan sebagai data pribadi yang bersifat spesifik bersama dengan data kesehatan, data genetika, data anak, catatan kejahatan, dan data keuangan pribadi. Pengelompokan tersebut menunjukkan bahwa pembentuk undang-undang menganggap data biometrik memiliki tingkat sensitivitas yang tinggi sehingga memerlukan perlindungan khusus.

Penjelasan Pasal 4 UU PDP menyebutkan bahwa data biometrik merupakan data yang berkaitan dengan fisik, fisiologis, atau karakteristik perilaku individu yang memungkinkan identifikasi unik terhadap seseorang, seperti gambar wajah, sidik jari, retina mata, dan DNA. Karakteristik unik tersebut menjadikan data biometrik sebagai identitas yang tidak dapat dipisahkan dari individu pemiliknya. Oleh karena itu, kebocoran atau penyalahgunaan data biometrik dapat menimbulkan risiko yang lebih besar dibandingkan kebocoran data pribadi umum.

Selain mengatur klasifikasi data biometrik, UU PDP juga memberikan sejumlah hak kepada subjek data pribadi. Hak tersebut meliputi hak memperoleh informasi mengenai penggunaan data pribadi, hak mengakses data, hak memperbaiki data, hak menarik persetujuan, dan hak mengajukan keberatan terhadap pemrosesan data tertentu. Hak-hak tersebut bertujuan memberikan kontrol kepada individu atas data pribadinya sehingga pemrosesan data dilakukan secara transparan dan bertanggung jawab.

Di sisi lain, pengendali data pribadi diwajibkan menjaga kerahasiaan, keamanan, dan integritas data yang diproses. Kewajiban tersebut mencerminkan penerapan asas kehati-hatian, pertanggungjawaban, dan kerahasiaan yang menjadi dasar perlindungan data pribadi di Indonesia.

Perlindungan Hukum terhadap Penyalahgunaan Data Biometrik dalam Sistem Hukum Indonesia

Perlindungan hukum terhadap penyalahgunaan data biometrik dapat dibedakan menjadi perlindungan preventif dan perlindungan represif. Perlindungan preventif dilakukan sebelum terjadinya pelanggaran hukum. Bentuk perlindungan ini diwujudkan melalui kewajiban memperoleh persetujuan dari subjek data, penerapan sistem keamanan informasi, pembatasan akses terhadap data biometrik, serta kewajiban pengendali data untuk menjaga kerahasiaan data pribadi. Tujuan utama perlindungan preventif adalah mencegah terjadinya penyalahgunaan data biometrik sejak awal proses pemrosesan data.

Sementara itu, perlindungan represif diberikan setelah terjadi pelanggaran terhadap data biometrik. UU PDP menyediakan berbagai instrumen penegakan hukum berupa sanksi administratif dan sanksi pidana. Sanksi administratif dapat berupa teguran tertulis, penghentian sementara pemrosesan data, penghapusan data, hingga denda administratif. Selain itu, undang-undang juga mengatur ketentuan pidana bagi pihak yang secara melawan hukum memperoleh, mengungkapkan, menggunakan, atau memalsukan data pribadi milik orang lain.

Namun demikian, efektivitas perlindungan hukum terhadap data biometrik masih menghadapi berbagai kendala. Pertama, perkembangan teknologi berlangsung lebih cepat dibandingkan perkembangan regulasi sehingga sering muncul bentuk-bentuk pemrosesan data baru yang belum diatur secara rinci. Kedua, kapasitas pengawasan dan penegakan hukum masih perlu diperkuat agar mampu mengimbangi kompleksitas kejahatan siber yang memanfaatkan data biometrik. Ketiga, kesadaran masyarakat mengenai pentingnya perlindungan data pribadi masih relatif rendah sehingga banyak pengguna layanan digital yang belum memahami risiko penggunaan data biometrik.

Saat ini AI dapat menimbulkan masalah terkait penyalahgunaan data pribadi. Data yang terkumpul dari berbagai platform sering digunakan untuk tujuan yang lebih luas, seperti iklan bertarget atau analisis perilaku, yang terkadang tidak sepenuhnya disetujui oleh pengguna. Hal ini berisiko (Kurniawan Tri Wibowo, Hukum Digital dan Privasi, 2025) mengarah pada eksploitasi data pribadi untuk keuntungan komersial tanpa memperhatikan hak privasi individu. Penyalahgunaan ini semakin diperburuk dengan potensi kebocoran data, baik akibat peretasan atau kelalaian dalam pengelolaan data oleh penyedia layanan. Keamanan data yang buruk dalam sistem AI dapat

mengakibatkan akses tidak sah oleh pihak ketiga, yang bisa mengekspos 129 individu pada risiko pencurian identitas atau penipuan.

Masalah lain yang muncul adalah bias dalam algoritma AI. Jika data yang digunakan untuk melatih model AI tidak representatif atau mengandung bias, maka hasil dari AI bisa memperburuk ketidaksetaraan atau diskriminasi terhadap individu atau kelompok tertentu. Misalnya, algoritma rekrutmen yang dilatih dengan data historis yang mencerminkan ketidaksetaraan gender atau rasial dapat menghasilkan keputusan yang diskriminatif, memperburuk ketidakadilan dalam dunia kerja. Selain itu, pengenalan wajah dan teknologi pelacakan lainnya dapat digunakan untuk mengumpulkan data biometrik secara terus-menerus, menambah risiko pengawasan massal yang dapat mengurangi kebebasan individu.

Ada beberapa langkah yang harus dilakukan dalam membuat Kebijakan Privasi terhadap data yang ada yang pertama adalah mengidentifikasi Jenis Data Pribadi yang akan dikumpulkan. Ada 2 data jenis data (Wibowo, 2025) yang dapat digolongkan yaitu Data Pribadi yang bersifat spesifik dan data pribadi yang bersifat umum Data pribadi yang bersifat spesifik mencakup Informasi Kesehatan, Biometrik, genetika, catatan kejahatan, data anak, data keuangan pribadi dan data lain yang sesuai dengan peraturan perundang – undangan. Dan data pribadi yang bersifat umum meliputi : Nama Lengkap, Jenis Kelamin, Kewarganegaraan, Agama, Status Perkawinan dan data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang, Setiap jenis data pribadi yang dikumpulkan harus dijelaskan secara rinci dalam kebijakan privasi, termasuk tujuan pengumpulannya. Misalnya, data dikumpulkan untuk Menentukan tunjangan karyawan, memberikan layanan Kesehatan diperusahaan, atau untuk tujuan penentuan strategi pasar dan marketing.. Selain itu, perusahaan juga harus memberikan informasi jelas mengenai bagaimana dan kapan data tersebut akan digunakan, serta jika data akan dibagikan dengan pihak ketiga, seperti mitra atau penyedia layanan kesehatan atau asuransi, dan dengan alasan yang sah.

Penting untuk menjelaskan langkah-langkah yang diambil oleh perusahaan untuk melindungi data pribadi tersebut, baik dari pencurian, kebocoran, atau akses yang tidak sah. Keamanan data menjadi aspek kunci dalam kebijakan privasi, yang mencakup penggunaan teknologi enkripsi, pengelolaan akses yang ketat, dan penerapan prosedur untuk mendeteksi serta merespons pelanggaran data. Perusahaan juga perlu menginformasikan kepada pengguna tentang hak-hak mereka terkait data pribadi, seperti hak untuk mengakses data, memperbaiki informasi yang salah, atau menghapus data yang sudah tidak diperlukan lagi. Selain itu, kebijakan privasi harus mencakup bagaimana perusahaan menangani permintaan pengguna untuk menarik persetujuan mereka dalam penggunaan data pribadi dan bagaimana perusahaan akan menanggapi permintaan tersebut sesuai dengan hukum yang berlaku.

Teori perlindungan hukum yang dikembangkan oleh Philipus M. Hadjon (2024) menempatkan kepastian hukum dan penghormatan terhadap hak-hak individu sebagai tujuan utama pembentukan hukum. Dalam konteks perlindungan data biometrik, teori tersebut mengandung makna bahwa negara tidak hanya berkewajiban membentuk regulasi yang mengatur pemrosesan data pribadi, tetapi juga harus memastikan tersedianya mekanisme pengawasan dan penegakan hukum yang efektif. Dengan demikian, perlindungan terhadap data biometrik tidak berhenti pada aspek normatif, melainkan harus diwujudkan melalui implementasi hukum yang mampu mencegah penyalahgunaan serta memberikan kepastian hukum bagi subjek data pribadi.

KESIMPULAN

Data biometrik merupakan data pribadi yang bersifat spesifik dan memperoleh perlindungan hukum khusus berdasarkan UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pengaturan tersebut menunjukkan bahwa negara mengakui tingginya tingkat sensitivitas data biometrik serta risiko yang dapat timbul apabila data tersebut disalahgunakan atau mengalami kebocoran.

Perlindungan hukum terhadap penyalahgunaan data biometrik dilakukan melalui mekanisme preventif dan represif. Perlindungan preventif diwujudkan melalui pengaturan hak subjek data dan kewajiban pengendali data dalam pemrosesan data biometrik. Sementara itu, perlindungan represif

dilakukan melalui penerapan sanksi administratif dan sanksi pidana terhadap pihak yang melakukan pelanggaran. Meskipun demikian, efektivitas perlindungan hukum masih menghadapi berbagai tantangan berupa perkembangan teknologi yang cepat, keterbatasan pengawasan, serta rendahnya kesadaran masyarakat mengenai pentingnya perlindungan data pribadi. Oleh karena itu, diperlukan penguatan regulasi teknis, peningkatan kapasitas pengawasan, dan edukasi masyarakat guna mewujudkan perlindungan data biometrik yang lebih efektif di Indonesia.

DAFTAR PUSTAKA

- Bambang Waluyo, *Penelitian Hukum Dalam Praktek*, Jakarta, Sinar Grafika, 1991
- Bernard Arief Sidharta, *Refleksi Tentang Struktur Ilmu Hukum (Sebuah Penelitian Tentang Fondasi Kefilsafatan dan Sifat Keilmuan Ilmu Hukum Sebagai Landasan Pengembangan Ilmu Hukum Nasional Indonesia)*, Mandar Maju, Bandung, 2013
- Kurniawan Tri Wibowo, *Hukum Digital dan Privasi Data*, Mataram, CV. Al-Haramain Lombok, 2025
- Soerjono Soekanto dan Sri Mamuji, *Penelitian Hukum Normatif (Suatu Tinjauan Singkat)*, Rajawali Pers, Jakarta, 2001
- Teddy Lesmana, *Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia*, Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia, 2022
- Philipus M. Hadjon, *Pengantar Hukum Administrasi Indonesia*, Gajah Mada University Press, 2024
- World Bank Group, *Technology Landscape for Digital Identification*, Washington D.C, Digital Impact Alliance, 2018