

TANTANGAN HUKUM PENGGUNAAN DATA BIOMETRIK DALAM KEPERLUAN BISNIS***¹Rian Mangapul Sirait, ²Roy Fachraby Ginting,****³Chris Dayanti Br. Ginting****^{*1,2,3}Universitas Audi Indonesia****^{*1,2,3}rhiandsiraid@gmail.com****Abstrak**

Penggunaan data biometrik semakin masif dalam berbagai sektor industri di Indonesia. Namun, penggunaan data biometrik ini juga menghadapi tantangan hukum yang signifikan terkait dengan perlindungan data pribadi. Tujuan dari penelitian ini adalah untuk mengidentifikasi dan menganalisis tantangan yang ditimbulkan oleh penggunaan teknologi biometrik dalam sektor bisnis di Indonesia serta mengeksplorasi kekurangan dalam Undang-Undang Perlindungan Data Pribadi yang ada saat ini. Penelitian ini menggunakan metode penelitian hukum normatif dengan meneliti bahan pustaka dan data sekunder yang mencakup aspek hukum dan literatur terkait perlindungan data pribadi. Pendekatan peraturan perundang-undangan digunakan untuk meneliti berbagai aturan hukum yang berkaitan dengan isu yang diangkat. Hasil dan pembahasan dari penelitian ini menunjukkan bahwa penggunaan data biometrik dihadapkan pada beberapa tantangan, termasuk risiko penyalahgunaan data, kerugian keuangan bagi perusahaan akibat gugatan ganti rugi dari subjek data, dan potensi pelanggaran hak privasi. Terdapat juga kekurangan dalam Undang-Undang Perlindungan Data Pribadi yang belum mencakup aturan mengenai tata cara mengajukan gugatan ganti rugi, hak subjek data dalam pemrosesan data, dan lembaga pelaksana perlindungan data pribadi. Kesimpulannya, diperlukan pembaruan dan peningkatan Undang-Undang Perlindungan Data Pribadi untuk mencakup aspek-atribut yang belum dicantumkan dan menangani tantangan hukum terkait data biometrik dalam bisnis di Indonesia. Selain itu, pembentukan lembaga pelaksana perlindungan data pribadi yang jelas dan efektif diperlukan untuk memastikan perlindungan yang baik bagi data biometrik dan menciptakan lingkungan bisnis yang lebih aman dan terpercaya di era digital yang semakin canggih.

Kata kunci: Data Biometrik, Perlindungan Data Pribadi, Hak**Abstract**

The use of biometric data is increasingly pervasive across various industries in Indonesia. However, this utilization also faces significant legal challenges concerning the protection of personal data. The purpose of this research is to identify and analyze the challenges posed by the use of biometric technology in the business sector in Indonesia, as well as to explore the deficiencies in the current Personal Data Protection

Law. This study adopts a normative legal research method, examining literature and secondary data covering legal aspects and relevant literature on personal data protection. A legislative regulation approach is used to investigate various legal rules related to the raised issues. The results and discussion of this research reveal that the use of biometric data is confronted with several challenges, including the risk of data misuse, financial losses for companies due to compensation claims from data subjects, and potential violations of privacy rights. There are also deficiencies in the Personal Data Protection Law that do not encompass regulations on the procedures for filing compensation claims, data subjects' rights in data processing, and the establishment of an effective institution for personal data protection. In conclusion, an update and enhancement of the Personal Data Protection Law are required to include the missing aspects and address the legal challenges concerning biometric data in Indonesian businesses. Additionally, the establishment of a clear and effective institution for personal data protection is necessary to ensure proper safeguarding of biometric data and create a safer and more trustworthy business environment in this everadvancing digital era.

Keywords: 3 Biometric Data, Personal Data Protection, Privacy Rights

PENDAHULUAN

Perkembangan teknologi yang sangat masif dari beberapa dekade belakangan mengubah pola transaksi manusia yang dulunya bersifat tradisional menjadi berbasis internet. Hadirnya teknologi memberikan perubahan yang signifikan pada berbagai aspek kehidupan manusia, khususnya aspek bisnis. Kemunculan internet sebagai akibat perkembangan teknologi menghubungkan dunia dalam skala global dan menghilangkan batasan fisik dalam transaksi bisnis. Adanya teknologi telah membuka kesempatan baru bagi bisnis untuk dapat bertumbuh dan bersaing dalam lingkungan yang semakin kompetitif. Bisnis dapat berkembang lebih pesat dengan memanfaatkan platform yang telah disediakan internet seperti e-commerce dan media sosial untuk menjangkau konsumen yang lebih luas, mencapai pertumbuhan yang berkelanjutan, dan menciptakan nilai tambah bagi para pelanggannya.

Perusahaan dalam melakukan persaingan bisnis harus melakukan langkah-langkah yang efektif dan efisien dalam menjangkau pelanggan demi meningkatkan pendapatan perusahaan dan menghemat pengeluaran. Langkah tersebut dapat dilakukan dengan cara memanfaatkan data. Saat ini data termasuk ke dalam faktor produksi dalam industri di era penggunaan data yang masif saat ini. Data dapat dikumpulkan, diproses, dikelola, dan didistribusikan kembali oleh pihak-pihak tertentu. Penggunaan data menjelma menjadi hal yang krusial dalam dunia bisnis karena dapat memberikan insight yang berguna bagi perusahaan untuk mengetahui customer behavior, market trend dan kinerja operasional perusahaan. Perusahaan dapat mengidentifikasi dan mengoptimalkan peluang bisnis sehingga menghasilkan keputusan yang lebih tepat. Data yang sering digunakan dalam mengidentifikasi peluang oleh perusahaan adalah data pribadi pelanggan. Penggunaan data pribadi pelanggan untuk melakukan optimalisasi kinerja perusahaan dalam melakukan bisnis dilakukan berdasarkan prinsip keamanan, kehati-hatian dan kerahasiaan data. Dewasa ini, jenis data yang relatif aman digunakan untuk menjaga keamanan dari segala bentuk ancaman pembobolan, penyalahgunaan dan penyelewengan penggunaan data adalah databiometrik.

Penjelasan Pasal 4 Ayat 2 Huruf b Undang-Undang Nomor 7 Tahun 2022 tentang Perlindungan Data Pribadi mendefinisikan data biometrik sebagai berikut: *“Yang dimaksud dengan “data biometric adalah data yang berkaitan dengan fisik, fisiologis, atau karakteristik perilaku individu yang memungkinkan identifikasi unik terhadap individu, seperti gambar wajah atau data daktiloskopi. Data biometrik juga menjelaskan pada sifat keunikan dan/atau karakteristik seseorang yang harus dijaga dan dirawat, termasuk namun tidak terbatas pada rekam sidik jari, retina mata, dan sampel DNA.”*

Data biometrik merupakan satu diantara data pribadi yang memiliki tingkat keamanan yang lebih tinggi dibandingkan dengan data lainnya karena memiliki keotentikan pada masing-masingnya. Data biometrik tidak terbatas pada aspek fisiologis semata (seperti: sidik jari, pola telapak tangan, mata, bentuk wajah, detak jantung dan sebagainya) melainkan juga mencakup kebiasaan individu seperti pola suara, gaya berjalan, dan pola kegiatan rutinitas lainnya. Data biometrik memberikan tingkat keamanan yang tinggi dan sulit untuk dibobol karena sifat keotentikan yang dimiliki sehingga data biometrik banyak digunakan beberapa tahun belakangan. Teknologi biometrik pada umumnya diperuntukan untuk proses otentikasi dan identifikasi individu. Proses otentikasi juga dikenal sebagai proses *one-to-one* yang dimana karakteristik biometrik individu dicocokkan dengan data mengenai individu tersebut yang telah tersedia di data base. Contoh penggunaan proses *one-to-one* ini dapat dijumpai pada saat membuka smartphone menggunakan sidik jari atau pengenalan wajah. Berbeda dengan proses identifikasi yang lebih dikenal dengan proses *one-to-many* dimana karakteristik biometrik individu yang tidak dikenal dibandingkan dengan data yang sejenis. Proses ini bertujuan untuk menghasilkan kemungkinan kecocokan, dan dengan demikian mengidentifikasi orang tersebut. Contoh penggunaan proses *one-to-many* dapat ditemukan pada sistem pengenalan wajah yang ada di Bandara.

Penggunaan data biometrik telah banyak digunakan dalam berbagai sektor industri. Industri yang telah mengadopsi pemanfaatan data biometrik, diantaranya seperti:

1. Industri transportasi. industri transportasi telah lama menggunakan data biometric seperti untuk keamanan bandara, dan banyak maskapai penerbangan kini menggunakan sistem penggunaan data biometrik untuk proses boarding.
2. Industri Perhotelan. Hotel mengadopsi teknologi pengenalan wajah dan pemindai sidik jari untuk mengoptimalkan prosedur check-in dan memberikan akses ke kamar.
3. Industri layanan keuangan dan e-commerce, biometrik telah menjadi elemen vital dalam platform keamanan melalui pemeriksaan biometrik melalui wajah, sidik jari, dan pola telapak tangan.
4. Industri Kesehatan. Penggunaan data biometrik pada industri Kesehatan dapat dilihat pada penggunaan gelang pintar yang digunakan untuk melacak detak jantung dan kadar oksigen secara terus menerus.
5. Industri otomotif. Industri otomotif menggunakan analisis wajah dan suara untuk mendeteksi keadaan fisik dan emosi pengemudi dan penumpang untuk menyesuaikan pengaturan kendaraan (misalnya, musik, pencahayaan, suhu).
6. Industri ritel. Industri ritel menggunakan data biometric dalam melakukan analisis wajah dan pelacakan perilaku diimplementasikan untuk memahami

preferensi pembeli, namu juga untuk mencegah kejahatan (misalnya, pencurian toko) dengan mendeteksi dan memberi peringatan perilaku mencurigakan.

Penggunaan data biometrik yang semakin masif di pelbagai industri menimbulkan tantangan yang signifikan dalam upaya perlindungan hukum bagi entitas yang terdaftar memiliki data biometrik pada suatu data base perusahaan atau organisasi. Tantangan tersebut harus dibarengi dengan infrastruktur aturan hukum yang memadai dan dapat melindungi masyarakat agar menimbulkan rasa aman dari potensi pembobolan data pribadi yang semakin hari marak terjadi. Indonesia telah memiliki aturan khusus mengenai perlindungan data pribadi, yaitu Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Realitas yang terjadi saat ini masih terdapat beberapa aspek penting yang belum dimuat dalam undang-undang Perlindungan data diantaranya yaitu: aturan mengenai tata cara mengajukan gugatan ganti rugi; hak subjek data dalam pemrosesan data pribadi; dan lembaga pelaksana perlindungan data pribadi. Berdasarkan permasalahan diatas, perlu dikaji lebih mendalam tentang Tantangan yang ditimbulkan dalam penyalahgunaan teknologi biometrik dalam sektor bisnis di Indonesia dan gambaran kekurangan aturan hukum mengenai penggunaan teknologi biometric dalam bisnis di Indonesia.

METODE

Metode yang digunakan dalam tulisan ini adalah penelitian hukum normatif, dimana penelitian yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder, bukan hanya mengkaji hukum dari segi peraturan perundang-undangan saja namun meliputi aspek yang lebih luas lagi dan dapat ditelusuri dari bahan kepustakaan. Pendekatan yang digunakan di dalam tulisan ini adalah pendekatan peraturan perundang-undangan yaitu meneliti berbagai aturan hukum yang berkaitan dengan isu yang diangkat. Adapun bahan hukum primer yang digunakan berkaitan dengan aturan hukum terkait data pribadi. Kemudian untuk bahan hukum sekunder berupa literatur atau buku, jurnal internasional dan nasional, serta literatur lainnya yang berkaitan dengan pembahasan perlindungan konsumen atas penyebarluasan data biometrik.

HASIL DAN PEMBAHASAN

A. Tantangan Penyalahgunaan Data Biometrik dalam Sektor Bisnis di Indonesia

1. Tantangan Bagi Perusahaan selaku Pengendali dan Prosesor Data

Tantangan yang harus dihadapi bagi perusahaan adalah adanya kerugian keuangan apabila terbukti melakukan penyalahgunaan data biometrik pemilik data. Pemilik data yang dalam hal ini adalah pengguna layanan atau pelanggan dapat mengajukan gugatan dan meminta ganti kerugian kepada perusahaan/organisasi apabila data yang dimiliki terbukti telah disalahgunakan. Hal tersebut telah terakomodir dalam Pasal 12 Ayat (1) Undang-Undang Perlindungan Data Pribadi.

Perusahaan/organisasi sebagai pihak pengendali data pribadi memiliki kewajiban untuk mencegah dan melindungi data pribadi dari pemrosesan yang tidak sah.¹³ Dampak bagi perusahaan selain kerugian keuangan yaitu potensi penurunan minat konsumen.¹⁴ Konsumen cenderung untuk menghindari layanan jasa atau produk suatu perusahaan yang memiliki permasalahan mengenai data. Penurunan minat konsumen dapat mempengaruhi kinerja perusahaan sehingga berpotensi menimbulkan kerugian bagi perusahaan secara materiil maupun nonmateriil.

Dampak lain yang dapat dirasakan oleh perusahaan yaitu adanya penurunan reputasi perusahaan yang mempengaruhi nilai investasi pada perusahaan. Salah satu faktor yang mempengaruhi minat investasi pada suatu perusahaan adalah bagaimana perusahaan menjaga reputasi yang dimilikinya. Adanya penurunan nilai investasi akan berpengaruh pada kondisi keuangan perusahaan dan dapat menurunkan kualitas operasional perusahaan.

2. Tantangan Bagi Subjek Data

Data biometrik berbeda dengan data pribadi lainnya, masing-masing data biometrik bersifat unik dan tidak mungkin sama dengan lainnya. Penanganan pemrosesan data biometrik memerlukan kehati-hatian karena data tersebut mampu merepresentasikan suatu entitas dengan akurat sehingga memiliki risiko yang tinggi apabila jatuh pada tangan yang salah. Oleh karena itu perusahaan harus memastikan bahwa data tersebut hanya digunakan sesuai dengan persetujuan yang sah dan sesuai peraturan yang berlaku.

Penanganan data biometrik perlu memperhatikan hak pribadi masing-masing entitas pemilik data. Hak pribadi yang dimaksud dalam Penjelasan Pasal 26 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik adalah hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan, hak untuk berkomunikasi dengan orang lain tanpa tindakan memata-matai dan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang. Penyalahgunaan data biometrik oleh perusahaan atau organisasi berpotensi menimbulkan pelanggaran etika yang serius. Dengan memiliki akses terhadap data biometrik konsumen, perusahaan dapat menciptakan ancaman terhadap privasi dan keamanan data individu. Misal, perusahaan dapat menggunakan data biometrik tanpa persetujuan untuk mengirim iklan yang tidak diinginkan dan mengganggu kehidupan konsumen. Selain itu, pengumpulan data biometrik juga memberikan wawasan mendalam tentang perilaku seseorang, yang dapat disalahgunakan oleh perusahaan untuk tujuan yang tidak etis, seperti penargetan produk atau layanan tanpa izin.

Dampak penyalahgunaan data biometrik yang lain yaitu potensi pelanggaran hak privasi. Hak privasi secara sederhana menurut Warren dan Brandeis dalam makalah Wahyudi Djafar yang berjudul “Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan” adalah hak untuk dibiarkan sendiri (*The Rights to be let alone*). Hak untuk dibiarkan sendiri yang dikemukakan oleh Warren dan Brandeis berdasarkan pada prinsip kehormatan pribadi dan nilai-nilai martabat individu.

Undang-Undang Dasar Negara Republik Indonesia menjamin adanya perlindungan terhadap privasi setiap warga negara, hal tersebut tertuang dalam Pasal 28 G Ayat (1) “perlindungan” yang dimaksud dalam pasal tersebut tidak hanya pada konteks sebagai hubungan langsung melainkan atas informasi dan data pribadi. Selain itu, aturan hukum mengenai perlindungan data pribadi juga tertuang dalam Undang-Undang Nomor 39 Tahun 2009 Tentang Hak Asasi Manusia Pasal 14 (2), 21 Pasal 29 (1) 22 dan Pasal 32.

Data Biometrik yang merupakan bagian dari data pribadi memiliki sifat yang sensitif. Data biometrik memerlukan transparansi dalam segala hal pemrosesannya,

dimulai dari saat pengumpulan data, penyimpanan, perbaikan, transfer dan penghapusan. Transparansi sangat diperlukan agar dapat mencegah penyalahgunaan dikemudian hari, misalnya Informasi biometric individu yang dikumpulkan secara diam-diam tanpa persetujuan dan partisipasi pengguna menimbulkan risiko pelanggaran privasi konsumen. Pengumpulan data biometrik individu dapat mengungkapkan informasi sekunder seseorang diluar dari tujuan pengumpulan data. Misal, dari pengambilan foto wajah seseorang dapat mengungkapkan informasi kesehatannya yang mungkin tidak ingin diungkapkan.

Contoh lain pelanggaran privasi yang dapat terjadi akibat penyalahgunaan data biometric yaitu adanya replikasi biometrik. Data biometrik pada awalnya memang merupakan data yang relatif aman, namun perkembangan kemampuan teknologi saat ini seperti meningkatnya resolusi kamera ponsel pintar, media yang mampu menampilkan video 4K dengan resolusi tinggi, penyimpanan data berbasis cloud, kecerdasan buatan dan machine learning meningkatkan risiko keamanan data secara signifikan. Munculnya teknologi baru tersebut sangat memungkinkan akan terjadinya replikasi biometrik yang apabila disalahgunakan akan dapat merugikan pemilik data yang bersangkutan.

B. Kekurangan Aturan Hukum Tentang Penggunaan Data Biometrik dalam Sektor Bisnis di Indonesia

Data pribadi dalam Undang-Undang Perlindungan Data Pribadi dibedakan menjadi dua, yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum. Data Biometrik termasuk kedalam data pribadi yang bersifat spesifik disamping data lainnya seperti data informasi Kesehatan, data genetika, catatan kejahatan, data anak, data keuangan pribadi dan data lainnya. Sedangkan data yang bersifat umum meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan dan data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

Undang-Undang Perlindungan Data Pribadi (UU PDP) secara garis besar mengkualifikasikan aktor yang terlibat dalam Pemrosesan data menjadi 4, yaitu Subjek data, Pengendali data, Prosesor Data dan Lembaga. UU PDP telah mengatur bagaimana hak dari subjek data, kewajiban dari Pengendali data dan prosesor data serta kewenangan lembaga dalam penyelenggaraan perlindungan data pribadi. Diantara 4 faktor tersebut, pengendali data dan prosesor data memiliki peranan yang signifikan dalam pemrosesan data. Pengendali data adalah pihak yang menentukan tujuan dan kendali pemrosesan data sedangkan prosesor data adalah pihak yang melakukan pemrosesan data atas nama pengendali data.

Kekurangan pertama UU PDP terkait tentang tata cara gugatan dan pengajuan ganti rugi. Pasal 12 Ayat (1) UU PDP menyatakan bahwa subjek data memiliki hak untuk menggugat dan meminta ganti kerugian. Namun aturan mengenai gugatan dan kerugian ini masih belum diatur dengan jelas terkait siapa yang bisa digugat apabila terjadi pelanggaran atau penyalahgunaan data,

khususnya data biometrik. Hal tersebut didasarkan adanya perbedaan istilah antara pengendali data dan prosesor data.

Secara kedudukan prosesor data mendapatkan kewenangan secara mandatoris dari pengendali data untuk melakukan pemrosesan data, dengan kata lain kedudukan pengendali data lebih tinggi daripada prosesor data dan tanggungjawab gugat berada pada pihak yang memberikan mandat yang dalam hal ini pengendali data. Dengan demikian hak untuk menggugat dan ganti rugi subjek data hanya dapat ditujukan kepada pengendali data sehingga pengendali data tidak dapat melimpahkan kesalahan kepada prosesor data. Selain pengendali data, pihak lain yang dapat digugat dan dimintai ganti kerugian oleh subjek data adalah lembaga yang berwenang yang ditugaskan melakukan perlindungan data pribadi apabila perumusan dan penetapan kebijakan dan strategi Perlindungan Data Pribadi yang dirancang oleh lembaga tidak mampu untuk dapat melindungi data pribadi khususnya data biometrik. Hal ini harusnya perlu dijelaskan dalam penjelasan Pasal 12 Ayat (1) atau aturan turunan dari UU PDP. Selain itu, masih belum terdapat mekanisme pengajuan gugatan baik terhadap pengendali data yang berada di Indonesia maupun pengendali data yang berada di luar negeri mengingat pelanggaran data pribadi khususnya data biometric bersifat cross-border yakni dapat melampaui batasan ruang administratif suatu negara.

Kekurangan kedua dalam UU PDP yakni terkait dengan hak subjek hukum yang belum terakomodir secara komprehensif. Subjek pribadi berhak untuk mendapatkan alternatif pilihan selain setuju dan tidak setuju dalam pengumpulan data pribadi. Pasal 20 Ayat (2) huruf a pada pokoknya menyatakan bahwa dalam melakukan pemrosesan data pribadi pengendali data wajib mendapatkan persetujuan yang sah secara eksplisit dari subjek data. Berdasarkan Pasal 20 Ayat (2) tersebut dapat dilihat bahwa subjek data hanya memiliki dua pilihan yaitu setuju dan tidak setuju. Kegiatan bisnis memerlukan adanya fleksibilitas dalam melakukan sebuah perjanjian dalam hal ini memerlukan perjanjian dalam pemrosesan data pribadi. Dalam hal perjanjian bisnis yang mensyaratkan data biometrik, subjek data harusnya dapat memilih alternatif pilihan selain setuju atau tidak setuju. Hal ini diperlukan, mengingat bahwa data pribadi berkaitan dengan hak privasi sehingga subjek data berhak untuk menyerahkan atau tidak menyerahkan data yang dimiliki kepada pihak lain.

Selain itu, dalam pengumpulan data pribadi khususnya data biometrik, pengendali data atau prosesor data memiliki syarat dan ketentuan tertentu. Subjek data dianggap telah memahami syarat dan ketentuan apabila menyetujui. Syarat dan ketentuan yang dimaksud pada dasarnya sebuah perjanjian elektronik yang berbentuk click-wrap agreement. Dalam click-wrap agreement, subjek data dianggap telah setuju apabila melakukan click pada bagian persetujuan (yang biasanya berisi: *I Accept, OK, I Agree, dll*).

Perjanjian click-wrap agreement ini umumnya muncul ketika seseorang ingin mengunduh perangkat lunak, mendaftarkan akun pada platform tertentu, dan sejenisnya. Sebagai konsekuensinya, subjek data harus mematuhi e-contract tersebut, namun terdapat masalah di dalamnya, terutama pada Syarat dan Ketentuan yang berisikan poin-poin yang dapat diartikan sebagai klausula eksonerasi (*exemption clause*).

Tujuan dari klausula eksonerasi ini adalah untuk membatasi atau bahkan menghapus tanggung jawab yang seharusnya ditanggung oleh pihak pengendali data. Dalam hal ini, klausula tersebut jelas merugikan pihak konsumen karena mereka dipaksa untuk tunduk pada aturan yang berdampak negatif bagi mereka, sementara sebaliknya menguntungkan pengendali data pribadi. Tidak adanya Hak subjek data untuk mendapatkan alternatif pilihan selain setuju dan tidak setuju membuat hak konsumen untuk mendapatkan perlindungan data pribadi khususnya data biometrik sebagaimana yang diperintahkan Undang-Undang sulit untuk terwujud.

Kekurangan lainnya terkait dengan UU PDP yaitu mengenai lembaga. Pada saat artikel ini ditulis (Agustus 2023), UU Perlindungan Data Pribadi (PDP) di Indonesia mengalami kekurangan terkait lembaga yang bertanggung jawab langsung atas penyelenggaraan perlindungan data pribadi. Pasal 58 UU PDP menyatakan bahwa penyelenggaraan perlindungan data pribadi dilaksanakan oleh lembaga yang bertanggung jawab kepada presiden. Namun, hingga saat ini, lembaga yang dimaksud dalam Pasal 58 belum terbentuk atau belum jelas keberadaannya.

Hal ini menyebabkan ketidakjelasan mengenai lembaga mana yang akan memiliki wewenang dan tanggung jawab langsung dalam menangani perlindungan data pribadi di Indonesia. Selain itu, kewenangan lembaga yang dimaksud oleh Pasal 58 memiliki irisan dengan lembaga lain yang juga terlibat dalam pengawasan dan perlindungan data pribadi, seperti Kementerian Komunikasi dan Informatika (Kemkominfo) dan Badan Siber dan Sandi Negara (BSSN).

Kemkominfo memiliki peran dalam mengawasi kebijakan, regulasi, dan standar teknis dalam bidang komunikasi dan informatika, yang mencakup aspek perlindungan data pribadi. Sementara itu, BSSN bertanggung jawab dalam mencegah, mengatasi, dan menangani ancaman siber, termasuk perlindungan data dari serangan siber. Ketidakjelasan mengenai pembagian kewenangan antara lembaga-lembaga terkait perlindungan data pribadi. Hal ini dapat menimbulkan tantangan dalam implementasi dan penegakan UU PDP, karena lembaga-lembaga tersebut harus bekerja sama secara efektif untuk melindungi data pribadi dengan tepat dan efisien.

Dalam mengatasi kekurangan ini, diperlukan langkah-langkah konkret untuk membentuk lembaga yang akan bertanggung jawab langsung atas penyelenggaraan perlindungan data pribadi, sesuai dengan amanat Pasal 58 UU PDP. Selain itu, diperlukan koordinasi yang lebih baik antara lembaga-lembaga terkait seperti Kemkominfo, BSSN, dan lembaga yang berwenang nantinya untuk memastikan ada pembagian tugas yang jelas dan efisien dalam melindungi data pribadi warga negara Indonesia. Upaya ini akan membantu menciptakan lingkungan yang lebih aman dan terpercaya dalam penggunaan data pribadi di Indonesia.

SIMPULAN

Penggunaan data biometrik dalam kegiatan bisnis di Indonesia menghadapi beberapa tantangan hukum. Data biometrik yang bersifat sensitif dan memiliki risiko tinggi apabila terjadi penyalahgunaan karena dapat mewakili individu secara akurat. Perkembangan teknologi yang semakin canggih membuat ancaman terhadap keamanan

data biometrik meningkat secara signifikan. Penyalahgunaan data biometrik dapat berdampak bagi perusahaan selaku pengendali data dan juga kepada individu selaku subjek data. Oleh karena itu, perlu adanya infrastruktur hukum yang memadai untuk menangani permasalahan tersebut.

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi masih terdapat beberapa hal krusial yang belum dicantumkan dalam Undang-Undang tersebut seperti: aturan mengenai tata cara mengajukan gugatan ganti rugi; hak subjek data dalam pemrosesan data pribadi; dan lembaga pelaksana perlindungan data pribadi. Saran untuk mengatasi tantangan hukum terkait penggunaan data biometrik dalam kegiatan bisnis di Indonesia meliputi pembaruan dan peningkatan UU PDP (Undang-Undang Nomor 27 Tahun 2022) dengan mencakup aspek-atribut yang belum dicantumkan, seperti aturan mengenai tata cara mengajukan gugatan ganti rugi dan hak subjek data dalam pemrosesan data pribadi. Selain itu, perlu segera membentuk lembaga pelaksana perlindungan data pribadi sesuai dengan amanat Pasal 58 UU PDP untuk menangani isu perlindungan data secara keseluruhan, termasuk data biometrik. Edukasi dan kampanye kesadaran tentang pentingnya perlindungan data biometrik harus dilakukan kepada masyarakat dan pelaku bisnis. Kerjasama dengan pihak ketiga yang memiliki standar keamanan yang

DAFTAR PUSTAKA

- Aguirre, E., Mahr, D., Grewal, D., Ruyter, K. De, & Wetzels, M. (2014). Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness. *Journal of Retailing*, 1–17. <https://doi.org/10.1016/j.jretai.2014.09.005>
- Anastasia, L., & Dewi, T. (2021). Analisis Ekonomi Terhadap Hukum dalam Kegagalan Perlindungan Data Pribadi Penggun E-Commerce. *Jurnal IUS Kajian Hukum dan Keadilan*. 9(3)
- Bayu Satrio, M., & Wih Widiatno, M. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia). *ICA of Law*, 1(1), 49–61.
- Bhatnagar, S., & Mishra, N. (2021). Conventional Biometrics and Hidden Biometric: A Comparative Study (pp. 473–481). https://doi.org/10.1007/978-981-15-7062-9_47
- Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, 37(3), 466–480. <https://doi.org/10.1016/j.ijresmar.2020.03.006>
- Chang, Y., Fan, S., Libaque-saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers ' perceived privacy. *Government Information Quarterly*, April, 1–15. <https://doi.org/10.1016/j.giq.2018.04.002>
- Djafar, W. (2019). Hukum Perlindungan Data Pribadi di Indonesia : Lanskap, Urgensi dan Kebutuhan Pembaruan. *Pasca Sarjana Fakultas Hukum Universitas Gajah Mada*, 1–14
- Firmansyah Putri, D. D., & Fahrozi, M. H. (2021). Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)
- Borneo Law Review, 5(1), 46–68. <https://doi.org/10.35334/bolrev.v5i1.2014>
- Fitriani, E. (Ed.). (2022). Kumpulan Policy Brief Universitas Indonesia Untuk Presidensi G-20 Indonesia 2022. Universitas Indonesia

- Ghoffar, A., Penelitian, P., & Pengkajian, D. A. N. (2019). Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital.
- Gibson, C., Kropotov, V., Lin, P. Z., Mcardle, R., Yarochkin, F., Kropotov, V., Lin, P. Z., & Mcardle, R. (2023). Leaked Today , Exploited for Life Affect Your Future. TrendMicro Research, 65–70.
- Hertianto, M. R. (2021). Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia Info Artikel. Kertha Patrika, 43(1), 93–109.
- Indriyani, M. (2017). Perlindungan Privasi dan Data Pribadi Konsumen Daring PadaOnline Marketplace System. Justitia Jurnal Hukum, 1(2).
<https://doi.org/10.30651/justitia.v1i2.1152>
- Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research : Accomplishments , challenges , and opportunities. Pattern Recognition Letters, 79(1), 80–105. <https://doi.org/10.1016/j.patrec.2015.12.013>
- Keyser, A. De, Bart, Y., Gu, X., Liu, S. Q., Robinson, S. G., & Kannan, K. (2021). Opportunities and challenges of using biometrics for business : Developing a research agenda. Journal of Business Research, 136(December 2020), 52–62.
<https://doi.org/10.1016/j.jbusres.2021.07.028>
- Khan, N., & Efthymiou, M. (2021). The use of biometric technology at airports: The case of customs and border protection (CBP). International Journal of Information Management Data Insights, 1(2), 100049.
<https://doi.org/10.1016/j.ijime.2021.100049>
- Kusuma, A. C., & Rahmani, A. D. (2022). Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia). SUPREMASI : Jurnal Hukum, 5(1), 46–63.
<https://doi.org/10.36441/supremasi.v5i1.721>
- Nafiaah, R. (2020). PELANGGARAN DATA DAN PENCURIAN IDENTITAS PADA ECOMMERCE. Cyberscurity Dan Forensik Digital, 3(1), 7–13. Jurnal JURISTIC Universitas Audi Indonesia Vol. 1, No. 2, Oktober 2021 e-ISSN: 2809-2287
- Novinna, V. (2020). Perlindungan Konsumen dari Penyebarluasan Data Pribadi oleh Pihak Ketiga : Kasus Fintech Peer To Peer Lending. Udayana Master Law Journal, 9(1), 92–110. <https://doi.org/10.24843/JMHU.2020.v09.i01.p07>
- Khairun Nisa, Chairina. (2022). Islam Studi Literatur Kejahatan Siber Pada Sistem Perbankan Syariah Di Era 4.0. Aghniya : Jurnal Ekonomi. 4(2), 218–224
- Ramadhan, P. S., Nurarif, S., Syahril, M., Riani, Y., & Gulo, N. (2022). Teknologi Biometrik Menggunakan Algoritma Eigenface Biometric Technology Using Eigenface Algorithm. Journal of Computing Engineering, System and Science (CESS), 7 (January), 43–54.
- Santoso, Z. Z. E., Krisdinanto, N., & Fiesta, B. R. S. (2023). Studi Netnografi Interaktivitas e-WOM pada Followers Twitter Tokopedia Pasca Krisis Kebocoran Data Pengguna. Jurnal Ilmu Komunikasi, 21(1), 1–23.
- Soemitra, A., & Adlina. (2022). Perlindungan Konsumen Terhadap Kebocoran Data Pada Jasa Keuangan Di Indonesia. Jurnal Insitusi Politeknik Ganesha Medan Juripol, 5, 288–303.
- Thalib, E. F., Putu, N., & Meinarni, S. (2019). Tinjauan yuridis mengenai marketplace berdasarkan peraturan perundang-undangan. Ius: Kajian Hukum Dan Keadilan, 7(2), 195–206. <https://doi.org/DOI: http://dx.doi.org/10.29303/ius.v7i2.622>
- Vidiana Girinda Wardani, Hedi Pudjo Santosa, D. S. (2023). Pengaruh Terpaan Berita Kebocoran Data Penduduk dan Terpaan Negative E-Word of Mouth di Media Sosial

- Terhadap Tingkat Kepercayaan Masyarakat Pada Pemerintah Pusat dalam Menangani Kasus Kebocoran Data. *Jurnal Fakultas Sosial Dan Politik Universitas Diponegoro*, 11(1), 1–10.
- Wang, F., & Filippi, P. De. (2020). Self-Sovereign Identity in a Globalized World : Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Hypothesis and Theory*, 2(January), 1–22. <https://doi.org/10.3389/fbloc.2019.00028>
- Weitzberg, K., Cheesman, M., & Martin, A. (2021). Between surveillance and recognition : Rethinking digital identity in aid. <https://doi.org/10.1177/20539517211006744>
- Wijayanti, A. A., Ariawan, I. G. K., & Udayana, H. U. (2021). Upaya Perlindungan Terhadap Identitas Para Pihak Dalam Praktik Cyber Notary. *Acta Vomitas Jurnal Hukum Kenotariatan*, 06(03), 679– 695. <https://doi.org/10.17977/um019v4i1p29-36>