

Kompleksitas Penggunaan *Face Recognition Technology* oleh PT Kereta Api Indonesia Ditinjau dari Aspek Perlindungan Data Pribadi dan Sistem Interoperabilitas

Suci Rizka Fadhillah^{1*}, Muhammad Shiddiq Putra¹

¹Ilmu Hukum, Fakultas Hukum, Universitas Andalas
Limau Manis, Kec. Pauh, Kota Padang, 25175.

Penulis untuk Korespondensi/E-mail: sucirizkafadhila@gmail.com

Abstract

The writing of this article aims to expose how the legal relationship between face recognition technology users and personal data protection, and how the application of an interoperability system between KAI face recognition and the Dukcapil database for user biometric data is intended to minimise irregularities in the personal data of KAI service users. This writing uses a juridical normative method. The paper uses secondary data collection methods and literature studies obtained from books, scientific journals, laws and regulations, and websites. The results of this writing show that there is a legal relationship between face recognition used by KAI and the protection of users' personal data in the form of biometric data that has been regulated in the Personal Data Protection Law (UU PDP). In addition to special regulations, a system is also needed that can help minimise the misuse of users' personal data, namely cooperation between KAI and Dukcapil, known as the interoperability system. This system has been implemented by several fields of agencies, such as banking, military, health, and education. Therefore, KAI is advised to use the interoperability system in the use of face recognition technology for the effectiveness and security of users' personal data.

Keywords: *Face Recognition Technology; KAI.; Personal Data Protection; Interoperability System.*

Abstrak

Penulisan artikel ini bertujuan untuk memaparkan bagaimana hubungan hukum antara pengguna face recognition technology dengan perlindungan data pribadi dan bagaimana penerapan jika diterapkan sistem interoperabilitas antara face recognition KAI dengan database Dukcapil terhadap data biometrik pengguna yang pada pokoknya dimaksudkan untuk meminimalisir terjadinya penyimpanan terhadap data pribadi pengguna jasa KAI. Penulisan ini menggunakan metode normatif yuridis. Penulisan ini menggunakan metode pengumpulan data sekunder dan studi kepustakaan yang diperoleh dari buku, jurnal ilmiah, peraturan perundangan, dan website. Hasil penulisan ini menunjukkan bahwa terdapat hubungan hukum antara face recognition yang digunakan oleh KAI dengan perlindungan data pribadi pengguna dalam bentuk data biometrik yang telah diatur dalam Undang-Undang Perlindungan Data Pribadi (UU PDP). Selain adanya regulasi khusus, diperlukan juga sebuah sistem yang dapat membantu meminimalisir terjadinya penyalahgunaan data pribadi pengguna, yaitu kerja sama antara KAI dengan Dukcapil yang dikenal dengan istilah sistem interoperabilitas. Adapun sistem ini telah diterapkan oleh beberapa bidang instansi, seperti bidang perbankan, militer, kesehatan, dan

pendidikan. Maka dari itu, KAI disarankan untuk menggunakan sistem interoperabilitas dalam penggunaan face recognition technology demi keefektifan dan keamanan data pribadi pengguna.

Kata kunci: *Face Recognition Technology; KAI; Perlindungan Data Pribadi; Sistem Interoperabilitas.*

PENDAHULUAN

Pada era teknologi saat ini, tidak ada hal yang tidak bisa dilakukan. Secara keseluruhan aktivitas sehari-hari dapat diselesaikan dengan menggunakan perangkat elektronik, seperti gawai modern atau lebih dikenal dengan istilah *gadget*. Namun, semua hal bisa menjadi *boomerang* jika tidak digunakan secara berhati-hati sebab dapat merugikan diri sendiri dan orang lain. Permasalahan terus bermunculan sejalan dengan perkembangan teknologi yang semakin menggila. Bisa dilihat dari barang sehari-hari saja, seperti alarm dengan berbagai bentuk suara atau *flowchart* absensi berbasis android (Setiawan, 2020). Meskipun teknologi membawa kemudahan bagi manusia sebab dapat membantu menyelesaikan hal yang tidak bisa dilakukan dengan cepat dan detail oleh tenaga biasa. Nyatanya, teknologi dapat menimbulkan efek negatif yang luar biasa dan ketergantungan oleh penggunanya. Untuk itu perlu adanya kewaspadaan dan kepekaan dalam menggunakannya.

Tidak hanya *gadget*, salah satu bentuk kecanggihan teknologi juga dimanfaatkan oleh PT Kereta Api Indonesia (KAI) sebagai suatu alat untuk mempermudah dan menghemat waktu pengguna, fitur tersebut dinamakan dengan *face recognition*. *Face recognition* merupakan sebuah teknologi buatan manusia yang mengakomodir pengenalan wajah pengguna yang dapat menganalisis secara cepat bagaimana karakteristik wajah seseorang (AWS, 2022). Alhasil, *face recognition* akan mengidentifikasi dan memverifikasi dengan cepat data diri seseorang yang menggunakan produk tersebut dengan menyesuaikan dengan data yang sudah diinput sebelumnya.

Kerja utama *face recognition* dengan cara mendeteksi terlebih dahulu bentuk wajah yang dilakukan dengan pengukuran secara detail dengan berbagai fitur wajah mulai dari bentuk mata, tulang pipi, kedalaman rongga mata, lebar hidung dan sebagainya. Hal ini dilakukan agar perangkat dalam mendeteksi wajah pengguna

dengan tepat dan rinci untuk keperluan beberapa aktivitas yang nantinya bertujuan untuk keamanan pengguna. Adapun beberapa fungsi dari hadirnya teknologi *face recognition* antara lain untuk mempermudah dan mempercepat proses kerja yang biasanya dilakukan secara manual. Hal inilah yang mendorong KAI untuk memanfaatkan teknologi ini

Tak hanya itu, *face recognition* juga dipergunakan dalam bertransaksi secara elektronik baik itu melalui *m-banking* ataupun *e-payment*. Evolusi dari penggunaan teknologi keamanan ini bahkan memiliki beberapa opsi yang ditawarkan kepada pengguna, antara lain kode PIN, sidik jari, termasuk yang terbaru *face recognition*. Diantara ketiga opsi yang muncul pengguna sepakat bahwa *face recognition* adalah opsi paling aman untuk diterapkan pada aplikasi transaksi *online* terlebih berkaitan dengan keuangan. Atas dasar ini pula, selain KAI banyak perusahaan yang memakai sistem presensi sidik jari dengan menggunakan biometrik wajah yang masif terhadap berbagai kegiatan perusahaannya. Tak ingin tertinggal, *Industri financial technology* terutama pada layanan pinjaman *online* juga mempergunakan teknologi *face recognition* ini sebagai salah satu cara untuk verifikasi pengguna secara cepat dan aman.

Terlepas dari beberapa kegunaan dibuatnya *face recognition*, ternyata memendam banyak risiko yang fatal bagi pengguna jika tidak mempertimbangkan keapasan dan kesialan yang dapat muncul. Sama halnya dengan potensi *Artificial Intelligence* (AI) pada umumnya memberikan manfaat teknologi yang luas bahkan dipergunakan untuk memitigasi perubahan iklim (Laza & Karo, 2023). Namun dapat menimbulkan risiko yang serius. Semua hal ini diperparah dengan ketiadaan regulasi khusus terkait perlindungan pengguna *face recognition* dalam menghadapi kerugian yang dialami, seperti pencurian data pribadi. Walaupun pada dasarnya telah ada regulasi yang mengatur perlindungan data pribadi, yakni Undang-Undang Nomor 27 Tahun 2022 tentang

Perlindungan Data Pribadi (UU PDP). Namun, untuk lebih spesifik terkait dengan dampak *face recognition* memang belum ada. Padahal *face recognition* tergolong sebuah *Artificial Intelligence* (AI) yang dipergunakan untuk mempermudah pengguna dalam menjalankan suatu kegiatan yang sudah banyak diterapkan di beberapa instansi di Indonesia.

Akan halnya UU PDP yang membantu mengakomodir perlindungan terhadap berbagai kegiatan, seperti pemrosesan dan penyimpanan data pribadi yang sejatinya sudah dijamin oleh konstitusi negara bahwa negara berhak atas perlindungan terhadap data pribadi warga negaranya. Maka dari itu, hadirnya UU PDP seakan menjawab permasalahan yang genting terkait dengan perlindungan data pribadi walaupun telah disinggung keharusannya pada Undang-Undang tentang Informasi dan Transaksi Elektronik (UU ITE). Ruang lingkup UU PDP tidak hanya melindungi data pribadi bersifat *online* tapi juga *offline*, seperti halnya nomor telepon di atas secarik kertas itu termasuk sebuah data yang bersifat *offline* (Rosadi, et al., 2018). Dengan begitu belum tercukupi penerapan dalam upaya pencegahan *cybercrime* terkait perlindungan data pengguna teknologi *face recognition* yang memungkinkan perusahaan ataupun sebuah komunitas bisnis untuk melakukan penyalahgunaan data pribadi pengguna demi keuntungan korporasi.

Di sisi lain, penggunaan akan *face recognition* memiliki beberapa keuntungan terutama dalam hal kepraktisan, yakni pengguna hanya mendongakkan wajah di depan mesin pemindai untuk melakukan verifikasi data (Verihubs, 2022). Selain itu, akurasi data dapat dikategorikan tinggi sebab kesalahan minimal terdapat pada pencocokan antara profil data pada *database* dengan bentuk wajah di layar mesin pendeteksi. Keunggulan lainnya sulit dipalsukan sebab profil wajah pengguna akan terverifikasi secara akurat dengan fitur *liveness detection* dapat mengetahui wajah asli atau topeng.

Ternyata, dibalik berbagai keuntungan yang ada jika menggunakan *face recognition* terselip beberapa ketidaksempurnaan fitur *touchless* satu ini, salah satunya pencurian data pribadi pengguna oleh pihak yang tidak bertanggung jawab yang dalam hal ini termasuk kategori delik aduan, jadi harus korban lah yang

melaporkan kejadian tersebut (Lidya, et al., 2020). Tak hanya KAI, berbagai perusahaan juga memakai fitur ini tentu awalnya sudah merekap dan menyimpan data pribadi pegawai atau karyawannya terlebih dahulu sebelum pegawai diperbolehkan menggunakan fasilitas *face recognition* di berbagai aktivitas di perusahaan.

Berdasarkan berbagai permasalahan tersebut, penulis tertarik membahas hubungan hukum antara penggunaan *face recognition technology* dengan perlindungan data pribadi pengguna serta penerapan sistem interoperabilitas antara *face recognition* KAI dengan *database* Dukcapil terhadap perlindungan data biometrik pengguna.

METODE PENELITIAN

Adapun metode yang digunakan dalam penulisan artikel ini, yaitu normatif yuridis. Adapun metode normatif, yakni penulisan yang berfokus pada sumber data sekunder sebagai data rujukan utama yang terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier (Benuf, 2020) sedangkan normatif yuridis adalah penulisan hukum dengan cara meneliti bahan kepustakaan atau data sekunder. Lebih lanjut, pendekatan yang digunakan dalam penulisan ini adalah pendekatan peraturan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Penulisan ini menggunakan metode pengumpulan data sekunder dan studi kepustakaan yang didapatkan dari buku, jurnal ilmiah, karya tulis, peraturan perundangan, dan website.

HASIL DAN PEMBAHASAN

Hubungan Hukum antara Penggunaan *Face Recognition Technology* dengan Perlindungan Data Pribadi Pengguna

Indonesia saat ini telah memiliki aturan hukum kontemporer terkait perlindungan data pribadi. Hal ini dijamin dalam UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Sebelum menelisik lebih jauh terkait perlindungan atas teknologi *face recognition* yang diterapkan oleh PT KAI terhadap konsumennya menurut UU PDP, perlu diketahui terlebih dahulu maksud dari data

pribadi beserta redaksi penyerta. Data pribadi menurut Pasal 1 angka (1) UU PDP adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Selanjutnya, terkait dengan perlindungan data pribadi menurut Pasal 1 angka 2 UU PDP adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi (UU PDP Pasal 1 angka 2). Informasi yang melekat pada data pribadi menurut Pasal 1 angka 1 UU PDP diartikan dalam Pasal 1 angka 3 sebagai keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik maupun nonelektronik (UU PDP Pasal 1 angka 3).

Pada dasarnya informasi yang melekat pada subjek data pribadi perlu dilindungi sebagai bentuk pemenuhan atas penjaminan hak konstitusional subjek data pribadi, sebab tergolong hal yang bersifat *private* dalam artian hal yang dijaga di mata publik (Rohmansyah, et al., 2023). Subjek data pribadi sendiri menurut UU PDP adalah orang perseorangan yang pada dirinya melekat data pribadi (UU PDP Pasal 1 angka 6). Data pribadi berdasarkan informasi didefinisikan sebagai objek yang dapat dirasakan oleh indera manusia. Selanjutnya, segala bentuk redaksional atas data pribadi tersebut, baik berupa perlindungannya, informasinya, hingga subjeknya diberikan jaminan perlindungan berdasarkan Pasal 4 ayat (2) UU PDP. Pasal ini menjelaskan bahwa terdapat perlindungan atas data pribadi masyarakat yang lebih spesifik, salah satunya adalah data biometrik (UU PDP Pasal 4 ayat 2). Data biometrik menurut undang-undang ini didefinisikan dalam penjelasannya sebagai 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.

Pada teknologi *face recognition*, wajah digunakan sebagai objek identifikasi. Wajah termasuk ke dalam fisik fisiologis dalam data biometrik yang dapat dianalisis menggunakan penginderaan manusia, yaitu dengan cara dilihat. Penggunaan wajah juga seharusnya dilindungi dalam data pribadi karena akan menganalisis dan menyimpan struktur fisik penggunaannya. Hanya saja, penggunaan teknologi *face recognition* yang mengidentifikasi wajah dapat dikecualikan menurut Pasal 15 ayat (1) UU PDP yang menyatakan bahwa hak dari subjek data pribadi dikecualikan untuk: kepentingan pertahanan dan keamanan nasional; kepentingan proses penegakan hukum; kepentingan umum dalam rangka penyelenggaraan negara; kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara; atau kepentingan statistik dan penelitian ilmiah (UU PDP Pasal 15). Dalam pasal ini dinyatakan dengan jelas bahwa hak subjek data pribadi dapat dikecualikan untuk beberapa kepentingan seperti yang disebutkan sebelumnya.

Hipotesis yang muncul adalah ketika pengaplikasian *face recognition* dalam sistem yang membantu pengguna KAI melewati pos *check in* sebelum menuju ke kereta api sudah menjamin atau belum mampu menjamin keamanan data pribadi biometrik pengguna. Pada dasarnya penggunaan *face recognition* memiliki dampak positif bagi pengguna KAI, salah satunya adalah mempermudah proses *boarding* KAI tanpa harus melakukan cetak tiket. Namun, hal ini menimbulkan suatu celah dimana penggunaan *face recognition* dalam sistem *boarding* oleh KAI belum menjamin adanya perlindungan keamanan data pribadi biometrik pengguna karena termasuk dalam bantuan sistem bayar.

Menurut Pasal 15 ayat (1) UU PDP, sistem pembayaran merupakan salah satu kepentingan yang tidak dilindungi dalam perihal data pribadi. Menurut Bank Indonesia, sistem pembayaran adalah sistem yang meliputi seperangkat regulasi, lembaga, dan mekanisme yang digunakan untuk melaksanakan transfer dana, guna memenuhi suatu kewajiban yang timbul

dari suatu kegiatan ekonomi (Bank Indonesia, 2024). Apabila *face recognition technology* dalam sistem *boarding* KAI digunakan, ada sedikit kerancuan apakah hal tersebut masuk ke dalam bantuan dalam sistem pembayaran atau justru urusan teknis saja. *Face recognition* dalam sistem *boarding* KAI dapat dikelompokkan sebagai suatu mekanisme yang pada dasarnya mempermudah penumpang untuk melanjutkan unsur prestasi atas transaksinya, yaitu dengan tanpa perlu mencetak tiket untuk masuk ke dalam kereta. Apabila terjadi kekosongan regulasi, maka belum tentu ada perlindungan terhadap data wajah pengguna yang memilih untuk menggunakan fitur ini, menimbang aturan dalam Pasal 15 ayat (1) UU PDP.

Di samping hal tersebut, UU PDP telah memberikan suatu kewajiban untuk penghapusan data pribadi, dalam hal ini wajah penumpang melalui teknologi *face recognition* oleh KAI dalam Pasal 43 ayat (1) UU PDP yang pada intinya menyampaikan bahwa pengendali data pribadi wajib menghapus data pribadi dalam hal: data pribadi tidak lagi diperlukan untuk pencapaian tujuan pemrosesan data pribadi; subjek data pribadi telah melakukan penarikan kembali persetujuan pemrosesan data pribadi; terdapat permintaan dari subjek data pribadi; atau data pribadi diperoleh dan/atau diproses dengan cara melawan hukum. Artinya, data wajah yang tersimpan oleh KAI dapat dihapus apabila memenuhi syarat sebagaimana yang disampaikan oleh amanat Pasal 43 ayat (1) UU PDP. Dalam kebijakan PT KAI, pengguna yang mendaftarkan dirinya dalam sistem *board face recognition* apabila tidak menggunakan fasilitas selama 1 (satu) tahun, maka data akan dihapus. Tandanya, terdapat mekanisme tersendiri dari PT KAI untuk menghapus data pribadi tersebut.

Selanjutnya, Pasal 44 ayat (1) UU PDP turut menyampaikan proses pemusnahan data pribadi. Maksud memusnahkan di sini berbeda dengan menghapus, yaitu tindakan untuk menghilangkan, melenyapkan, atau menghancurkan data pribadi sehingga tidak lagi dapat digunakan untuk mengidentifikasi subjek data pribadi. Dalam Pasal ini, pada intinya menjelaskan bahwa pengendali data pribadi wajib memusnahkan data pribadi dalam hal: telah habis masa retensinya dan berketerangan dimusnahkan berdasarkan jadwal retensi arsip;

terdapat permintaan dari subjek data pribadi; tidak berkaitan dengan penyelesaian proses hukum suatu perkara; dan/atau data pribadi diperoleh dan/atau diproses dengan cara melawan hukum. Artinya adalah UU PDP telah mewajibkan bagi seluruh prosesor data pribadi untuk memusnahkan data pribadi agar tidak dapat mengidentifikasi subjek data pribadi lagi. Dalam hal ini, PT KAI sebagai prosesor data pribadi pengguna turut wajib memusnahkan data pribadi, seperti dengan kebijakan penghapusan atau retensi data wajah *face recognition* pengguna yang tidak menggunakan fitur tersebut selama 1 (satu) tahun.

Penerapan Sistem Interoperabilitas antara *Face Recognition* KAI dengan Database Dukcapil terhadap Perlindungan Data Biometrik Pengguna

Dalam menggunakan fitur *face recognition* KAI seorang pengguna diharuskan untuk melakukan pendaftaran terlebih dahulu, hal ini tentu menjadi krusial untuk dipikirkan oleh pengguna karena menyangkut keamanan data pribadinya. Lagi pula, persoalan data biometrik tergantung dari interoperabilitas yang ada pada sistem. Sebab data biometrik dalam hal ini mencakup semua data pribadi yang tertera saat hanya melihat wajah saja bukan berarti wajah termasuk objek 3D (Lin, 2000). Interoperabilitas adalah proses yang menghubungkan beberapa aplikasi perangkat lunak sebagai layanan (AWS, 2023). Adapun data biometrik sendiri menurut UU PDP merupakan data yang berkaitan dengan hal fisik, fisiologis, atau karakteristik perilaku individu yang memungkinkan untuk identifikasi unik terhadap individu, seperti gambar wajah atau daktiloskopi, termasuk penggunaan mesin yang memverifikasi sidik jari, retina mata, sampel DNA (UU PDP Pasal 4 ayat (2) huruf b). Tentu perihal seputar wajah akan terdeteksi melalui penggunaan *face recognition* termasuk salah satu pelayanan PT KAI dalam hal registrasi ulang penumpang tanpa perlu mencetak tiket kembali.

Permasalahan terkait dengan data biometrik dialami oleh PT KAI terkait dengan penggunaan *face recognition* saat penumpang ingin melakukan *boarding*. Namun, data biometrik hasil pindaian mesin *face recognition* tersebut tidak jelas aturan keamanannya. Walaupun *VP Public Relation* PT KAI telah menjelaskan bahwa data pribadi penumpang yang melakukan *face recognition* akan disimpan hanya selama

jasa KAI digunakan oleh penumpang, ketika jasa tidak dipakai dalam waktu setahun maka pihak KAI akan menghapus data tersebut secara permanen (Bestari, 2023). Tentu hal ini menjadi pertimbangan yang serius bagi pengguna terkait nantinya terjadi penyalahgunaan data pribadi.

Semenjak teknologi ini digunakan dengan tujuan mempermudah pengguna dalam melakukan pendaftaran saat ingin *boarding*, beberapa orang yang memiliki kesadaran terhadap pentingnya data pribadi akan menolak melakukannya dan memilih untuk memakai cara manual. Pada dasarnya memang cara manual lebih lama karena memakan waktu lebih panjang daripada sekedar menyodorkan wajah ke mesin *face recognition*. Sebab teknologi verifikasi wajah sejatinya tidak membutuhkan tenaga manusia yang mempergunakan sistem kontrol akses, identifikasi ulang, dan evaluasi independen (Wang & Deng, 2021). Banyak pendapat yang berseliweran terkait hal ini, ada yang menyarankan bahwa PT KAI harusnya bekerja sama dengan instansi lain termasuk Kependudukan dan Pencatatan Sipil (Dukcapil) di daerah tersebut. Hal ini dapat meminimalisir pekerjaan KAI yang tidak pada posisi sebagai penyimpan dan pemrosesan data pribadi. Setelah itu, data dari pihak KAI hasil *face recognition* pada penumpang akan disamakan dengan *database* yang ada di Dukcapil, sebab lisensi seluruh data penduduk termasuk rekam wajah dipegang oleh lembaga tersebut. Dalam artian, cukup Dukcapil saja yang menyimpan data pribadi penumpang bukan pihak KAI.

Kolaborasi antara kedua instansi tersebut dapat disebut dengan sistem interoperabilitas. Sistem interoperabilitas merupakan suatu sistem yang harus dimiliki sistem KAI agar keamanan data pengguna jasa layanan KAI dapat terus terjaga dengan cara tetap berkoordinasi dengan Dukcapil untuk penyimpanan data. Sebab, sistem interoperabilitas memungkinkan data yang dikelola oleh unit yang berbeda untuk digunakan bersama agar pengambilan keputusan menjadi lebih cepat dan baik. (Faisal, 2014). Selain itu, perlu adanya pengembangan lebih lanjut pada sistem ini agar nantinya kombinasi keduanya dapat menghasilkan pelayanan yang baik bagi pengguna KAI, sebab interoperabilitas sendiri mengacu pada standar, protokol, teknologi, dan mekanisme yang memungkinkan data mengalir di antara kedua sistem dengan segala intervensi manusia yang minimal (AWS,

2022). Dengan adanya sistem interoperabilitas membantu beberapa komunitas atau perusahaan dalam mencapai efisiensi dalam hal pendataan sehingga menawarkan layanan yang lebih berkualitas dan meningkatkan kepercayaan masyarakat.

Jika nantinya terdapat permasalahan terkait dengan data penumpang, haruslah diurus oleh KAI sebagai pihak penyelenggara. Beda hal jika KAI dan Dukcapil memutuskan untuk menggunakan sistem interoperabilitas yang memaknai bahwa kedua pihak harus bertanggung jawab. Namun, pemrosesan data pribadi akan ditekankan pada pihak Dukcapil sesuai dengan Pasal 1 ayat 4 UU PDP, yakni prosesor data pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri atau bersama dalam melakukan pemrosesan data pribadi. Lebih lanjut, kewenangan dari pemrosesan data pribadi meliputi pemerolehan dan pengumpulan, pengolahan dan penganalisisan, penyimpanan, perbaikan dan pembaharuan, serta beberapa tugas lainnya yang sebagaimana yang tercantum dalam Pasal 16 UU PDP, semuanya akan tertuju pada Dukcapil.

Untuk itu, ketika ada pembobolan data pribadi penumpang oleh pihak KAI yang sudah tercantum pada Dukcapil, pertanggung jawaban akan ada pada Dukcapil sebab KAI hanya menyediakan opsi layanan *face recognition* untuk mempermudah proses *boarding* saat verifikasi data penumpangnya sehingga tidak perlu menunjukkan berbagai dokumen seperti *e-boarding pass*, Kartu Tanda Penduduk (KTP), dan dokumen lainnya (Wibawana, 2023). Jika penumpang tidak bersedia, maka dapat memakai proses manual saja. Opsi menggunakan *face recognition* hanya diperuntukkan bagi mereka yang percaya atas keamanan data oleh KAI. Untuk itu, KAI perlu melakukan upaya lebih gencar dengan memberikan jaminan terkait dengan data pribadi yang dipindai melalui *face recognition* tersebut agar para penumpang tidak was-was.

Pembobolan dan pencurian data pribadi semakin marak terjadi, inilah salah satu alasan penumpang menjadi lebih waspada. Sebab bagaimanapun kedua hal tersebut termasuk tindak pidana, baik disengaja (*intentional threats*) maupun tidak disengaja (*inadvertent threats*) (Suryanto, et al., 2024). Tak heran, hal

ini banyak terjadi di Indonesia menimbang teknologi yang mumpuni untuk mengantisipasi hal tersebut belum masif. Adapun regulasi yang mengatur terkait perlindungan data pribadi baru diundangkan pada 2022 lalu setelah adanya kasus pencurian data pribadi *e-commerce* Tokopedia yang kehilangan 90 juta lebih data pengguna, tak hanya pada *e-commerce* kebocoran data juga marak terjadi pada *website* pemerintah (Supriyanti, 2024). Semua kasus tersebut berakar dari lemahnya sarana pengamanan dan minimnya regulasi yang ada saat itu. Jadi, dapat disimpulkan fasilitas *face recognition* yang disediakan oleh KAI sejatinya sangat mempermudah dalam melakukan verifikasi penumpang, namun perlu dilakukan peningkatan terhadap keamanan data pribadi dengan cara mengadakan kerjasama dengan Dukcapil melalui sistem interoperabilitas, agar dapat mengantisipasi terjadinya kebocoran data yang signifikan.

Adapun menurut *US Government Accountability Office* yang dibutuhkan untuk melakukan *face recognition*, yakni kamera, *face print*, *database*, dan algoritma untuk membandingkan target dengan *face print* dalam *database* (Mutiara, 2022). Berdasarkan hal tersebut, kerja sama antara KAI dengan Dukcapil nantinya dapat lebih efektif dengan adanya pembagian tugas. Pihak KAI bertugas dalam menyediakan fasilitas *face recognition* yang nantinya akan dihubungkan dengan *database* seluruh penduduk yang dikelola oleh Dukcapil cabang wilayah tersebut. Pihak KAI tidak perlu menyimpan data penumpang dan merasa khawatir akan terjadi pembobolan data. Kerjasama ini telah dicoba oleh beberapa lembaga terkhusus dalam hal inovasi teknologi, seperti perbankan, militer, kesehatan, dan pendidikan.

Tentunya dalam rangka peningkatan inovasi dalam lingkup teknologi, sistem interoperabilitas ini mendapat dukungan dari pemerintah. Hal ini dibuktikan dengan hadirnya Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 7 Tahun 2013 yang menjadi salah satu bukti keseriusan pemerintah dalam mendukung penerapan interoperabilitas demi meningkatkan kualitas layanan publik. Dengan adanya sistem ini dapat menjadikan kolaborasi objek yang berbeda yang memungkinkan data atau informasi sehingga dapat ditukarkan antar sistem satu dengan

lainnya, seperti menggunakan protokol HTTP atau jaringan TCP/IP. Tak hanya itu, sistem ini sudah diatur secara khusus dalam Peraturan Pemerintah Nomor 82 Tahun 2012 Pasal 13 terkait dengan Implementasi Interoperabilitas. Pada dasarnya tujuan utama sistem ini berfokus pada efektivitas layanan dan rasa puas pengguna, tak lupa sebuah persembahan inovasi baru terhadap dunia teknologi (Akbar, 2023).

Perbankan termasuk instansi yang telah menerapkan sistem interoperabilitas ini, pada 28 Juni 2022 silam yang melakukan kolaborasi terkait dengan interoperabilitas data sekaligus layanan perbankan antara Bank Mandiri, Bank Negara Indonesia, dan Bank Rakyat Indonesia. Sistem ini diterapkan dengan maksud peningkatan kualitas pelayanan wajib pajak dengan memanfaatkan teknologi. Tentunya, sistem interoperabilitas memungkinkan terjadinya pertukaran data atau informasi melalui perantara penyedia kanal atau *website* berbayar. Dengan berbagai keuntungan yang didapatkan oleh perbankan diantaranya meningkatkan proteksi privasi, penyediaan data yang berkualitas, mengurangi pengeluaran, dan meningkatkan kepuasan pengguna (Srinadi, 2022). Sistem ini juga diterapkan pada bidang pendidikan dengan menggunakan STB sebagai terobosan baru yang digunakan pada *smart TV* dan komputer (Akbar, 2023). Maka berdasarkan pertimbangan di atas, tidak ada alasan untuk tidak menerapkan sistem interoperabilitas pada fasilitas *face recognition* KAI dan *database* dari Dukcapil demi meminimalisir terjadinya *cybercrime* terhadap data pribadi pengguna demi mendapatkan segudang keuntungan.

KESIMPULAN

Pada dasarnya semua data pada subjek data pribadi perlu dilindungi sebagai bentuk jaminan dari hak konstitusional subjek data pribadi sesuai dengan Pasal 1 angka (6) UU PDP yang memaknai bahwa orang perseorangan yang pada dirinya melekat data pribadi. Data pribadi didefinisikan sebagai objek yang dapat dirasakan oleh indera manusia. Hal ini diperjelas oleh Pasal 4 ayat (2) UU PDP yang disinggung bahwa terdapat perlindungan atas data pribadi masyarakat yang lebih spesifik, salah satunya adalah data biometrik. Untuk itu, data biometrik yang disimpan oleh KAI dalam pemrosesan data

pengguna dengan memanfaatkan fasilitas *face recognition* perlu diadakan aturan yang lebih kompleks membahas tentang teknologi baru ini sekaligus pertanggungjawaban pihak penyedia fasilitas demi menjamin perlindungan data pribadi pengguna. Sebab bagaimanapun, data pribadi pengguna termasuk data yang *private* demi menjaga integritas dan martabat pribadi seseorang (Saragih, et al., 2020).

Hal ini salah satu upaya mengantisipasi terjadinya *cybercrime* dalam penerapan *face recognition*. Atas dasar itu, perlu diberlakukan sistem interoperabilitas antara fitur *face recognition* dari KAI dengan *database* dari Dukcapil. Sistem ini telah ampuh diterapkan pada beberapa bidang kegiatan pemerintahan, mulai dari perpajakan, militer, kesehatan, dan pendidikan, sebab kerjasama antar beberapa instansi yang berkaitan dengan pengelolaan data telah terbukti membawa keuntungan, seperti meningkatkan proteksi privasi, penyediaan data yang berkualitas, mengurangi pengeluaran, dan meningkatkan kepuasan pengguna.

REFERENSI

- Akbar, N. M., Putra, F. P. E., Imam, K. Z., & Mansyur, M. U. (2023). "Analisis Kinerja dan Interopabilitas STB Sebagai Server Penilaian Akhir Tahun". *Jurnal Informasi dan Teknologi*, Vol. 5 No. 2, 91-96.
- AWS. "Apa Itu Interoperabilitas?" Diakses pada 19 Juni 2024 di halaman <https://aws.amazon.com/id/what-is/interoperability/>
- Bank Indonesia. "Fungsi Utama Sistem Pembayaran." Diakses pada 19 Juni 2024 di halaman <https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/default.aspx>
- Benuf, Kornelius. (2020). "Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer" *Jurnal Gema Keadilan*. Volume 7 Edisi 1.
- Bestari, Novina Putri. (2023). "Face Recognition di Stasiun KAI Langgar Hukum dan Privasi". 22 Nov 2023. Diakses pada 19 Juni 2024 di halaman <https://www.cnbcindonesia.com/tech/20231122082939-37-490932/face-recognition-di-stasiun-kai-langgar-hukum-dan-privasi>
- Faisal, Muhammad. (2014). "Implementasi Model Interoperabilitas Pada Sistem Informasi Akademik Berbasis Multiplatform" *Jurnal PROGRES*. Vol. 6 No. 2.
- Indonesia (2012). Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
- Indonesia (2018). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Indonesia (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Kementerian Komunikasi dan Informatika. (2013). Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 7 Tahun 2013 tentang Pedoman Penerapan Interoperabilitas Dokumen Perkantoran Bagi Penyelenggara Sistem Elektronik Untuk Pelayanan Publik.
- Laza, Jeremiah Maximillian dan Rizky Karo Karo. (2023). "Perlindungan Hukum terhadap Artificial Intelligence dalam Aspek Penyalahgunaan Deepfake Technology pada Perspektif UU PDP dan GDPR" *Jurnal Lex Prospicit*, Vol.1, No. 2.
- Lin, Shang-Hung. (2000). "An Introduction to Face Recognition Technology" *Informing Science Special Issue on Multimedia Informing Technologies*. Vol. 3 No. 1.
- Mutiara, Monica. (2022). "Cara Kerja Face Recognition". sis.binus.ac.id, 5 Jan 2022. Diakses pada 20 Juni 2024 di halaman <https://sis.binus.ac.id/2022/01/05/cara-kerja-face-recognition/>
- Rohmansyah, Duta Agung, dkk. (2023). "Urgensi Perlindungan Hak Asasi Anak Atas Data Pribadi di Era Digitalisasi Berdasarkan Prinsip Negara Hukum." *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam*.
- Rosadi, Sinta Dewi dan Garry Gumelar Pratama. (2018). "Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia" *Veritas et Justitia*, Vol. 4, No. 1.
- Saragih, Lydia Kharista dkk. (2020). "Perlindungan Hukum Data Pribadi terhadap Penyalahgunaan Data Pribadi pada Platform Media Sosial" *Jurnal Hukum De'rechtsstaat*, Vol. 6, No. 2
- Setiawan, Panji R. (2020). "Aplikasi Absensi Online Berbasis Android" *IT Journal Research and Development (ITJRD)* Vol. 5 No. 1: Hal 63-69.

- Srinadi, Ni Putu Deva. "Interoperabilitas Sistem Bagi Layanan Perpajakan." www.pajakku.com, 1 Ags 2022. Diakses pada 20 Juni 2024 di halaman <https://www.pajakku.com/read/62d61804a9ea8709cb18b134/Interoperabilitas-Sistem-Bagi-Layanan-Perpajakan->
- Supriyanti, Nadila Marta. (2024). "Perlindungan Hukum Atas Kerahasiaan Data Wajib Pajak dalam Proses Validasi Melalui E-PHTB Notaris." Universitas Islam Sultan Agung.
- Suryanto, Dasep., dkk. (2024). "Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam Industri Ritel Tinjauan terhadap Kepatuhan dan Dampaknya pada Konsumen" Jurnal Veritas, Vol. 10 No. 1.
- Verihubs. (2022). "Pertimbangkan Kelebihan dan Kekurangan Face Recognition Ini". Verihubs.com, 16 Okt 2022. Diakses pada 22 Juni 2024 di halaman <https://verihubs.com/blog/kelebihan-dan-kekurangan-face-recognition>
- Wang, Mei and Weihong Deng. (2021). "Deep Face Recognition: A Survey" *Neurocomputing* Vol. 429. Pages 215-244.
- Wibawana. (28 Desember 2023). "Face Recognition KAI ada di Stasiun Mana Saja Simak Daftarnya." Diakses pada 20 Juni 2024 di halaman <https://news.detik.com/berita/d-7112316/face-recognition-kai-ada-di-stasiun-mana-saja-simak-daftarnya>