Biblioteca del Congreso Nacional de Chile / BCN
Asesoría Técnica Parlamentaria
Mayo 2024

Tecnologías de reconocimiento facial en el control migratorio. Derecho Comparado.

Autores

Paola Alvarez D.
Pedro Guerra.

Email: palvarez@bcn.cl

Comisión

Elaborado para la Comisión de Gobierno Interior, Nacionalidad, Ciudadanía y Regionalización de la Cámara de Diputadas y Diputados.

Nº SUP: 141331

Resumen

El presente informe analiza el uso y regulación de las tecnologías de reconocimiento facial (*Facial Recognition Technology*, FRT) como mecanismo de control migratorio en el derecho comparado. La FRT, a diferencia de la tecnología biométrica, puede cumplir dos funciones: (1) la identificación de una persona para verificar quién dice ser (verificación uno-a-uno) y (2) identificación de una persona entre un grupo de individuos, en un área, imagen o base de datos específica (identificación uno-a-muchos). Son las únicas funciones que se pueden asignar al FRT y sus posibles consecuencias en su uso las que justifican una regulación especial.

El uso de FRT está intrínsecamente vinculado al procesamiento de datos personales, particularmente los datos biométricos en su calidad de datos sensibles. Además, tiene un impacto directo o indirecto en una serie de derechos fundamentales. Por lo tanto, cualquier uso de FRT debe realizarse en estricto cumplimiento del marco legal aplicable, que actualmente en Chile corresponde a la Ley N° 19.628 sobre protección de la vida privada (que, de aprobarse, será reemplazada por proyecto de ley que regula la protección y el tratamiento de datos personales y crea la Agencia de Protección de Datos Personales, Boletín 11.092-07 y 11.144-07, refundidos).

Asimismo, esta tecnología acarrea riesgos tanto técnicos (errores de identificación o falsos positivos/negativos) como jurídicos. Lo anterior por cuanto, si bien la FRT se utiliza principalmente entre los organismos encargados de hacer cumplir la ley con fines de verificación de identidad (ej. control migratorio), su uso más controvertido es aquél realizado para vigilancia (masiva), especialmente en espacios de acceso público. Este uso generalmente se encuentra prohibido por violar las garantías fundamentales del derecho a la privacidad y a la no discriminación.

Impulsados por actos de terrorismo y la pandemia de COVID-19, países como EE.UU., Australia y Nueva Zelanda han implementado sistemas de control migratorio que usan la biometría en general (ej. huellas dactilares) y la FRT en particular, para fines de verificación (a través de *ePassports*) así como de identificación en aeropuertos. Todo lo anterior en contextos de cooperación internacional e intercambio de información entre países que implementado la tecnología señalada. En cambio, el uso gubernamental de la FRT en la Unión Europea se encontraría limitado por el Reglamento General de Protección de Datos, más restrictiva en cuanto a la protección de los datos personales y la posibilidad de usarla para fines de identificación masiva.

Introducción

En los últimos años, los sistemas o tecnologías de reconocimiento facial (*facial recognition technology*, FRT) han acelerado su crecimiento en escala y alcance, y se están convirtiendo en una parte cada vez más omnipresente de nuestra vida diaria. Como resultado, la mayoría de los ciudadanos de los países más poblados del mundo ya están inscritos en uno o más sistemas de reconocimiento facial[1], lo sepan o no (Wenger et al., 2023).

En el marco de la discusión de materias relacionadas con la migración irregular y su control en la Comisión de Gobierno Interior, Nacionalidad, Ciudadanía y Regionalización de la Cámara de Diputadas y Diputados, el presente informe analiza el reconocimiento facial biométrico como mecanismo de control en materia de migración, en Chile y el derecho comparado.

Para responder a esta solicitud se revisaron las experiencias y normativas de otros países, así como la prensa internacional en busca de noticias dando cuenta de una medida de esta índole, con el fin de obtener antecedentes para orientar la búsqueda. Se corroboró la información de prensa con fuentes gubernamentales de cada país.

El documento se estructura en cuatro capítulos: en el primero se definen y describen los sistemas de reconocimiento biométrico facial para el control de la inmigración; en el segundo se analiza la tendencia regulatoria internacional de protección de datos biométricos; en el tercero se describe el estado de la cuestión en Chile, identificando iniciativas sobre la materia, así como el marco legal que le es aplicable al problema en la actualidad y los límites que existen en relación con la protección de datos; mientras el cuarto se refiere a la experiencia comparada de algunos países en los que se utilizan este tipo de tecnologías para el control migratorio.

El tema que aborda este informe y sus contenidos están delimitados por los parámetros de análisis acordados, por el plazo de entrega convenido y por la información disponible. No es un documento académico y se enmarca en los criterios de neutralidad, pertinencia, síntesis y oportunidad en su entrega. Las traducciones son propias.

[1] Por ejemplo, en Estados Unidos, casi 200 millones de residentes ya están inscritos en la base de datos de reconocimiento facial del FBI, que se creó aprovechando el acceso de esta agencia a las fotografías de las licencias de conducir en muchos estados. En China, un sistema de vigilancia utiliza el reconocimiento facial para monitorear el comportamiento civil y hacer cumplir el sistema de puntuación de crédito social. En Rusia, las autoridades adquirieron más de 100.000 cámaras en Moscú para construir un sistema de aplicación de la cuarentena por COVID, basado en reconocimiento facial (Wenger et al., 2023).

I. Reconocimiento facial biométrico como mecanismo de control de la seguridad[2]

1. ¿Qué es la tecnología de reconocimiento facial?

El reconocimiento facial es un proceso técnico de identificación que se desarrolla mediante tecnologías muy comunes en la vida diaria, que están presentes en sistemas de controles de acceso (por ejemplo, a edificios de empresas u oficinas gubernamentales), documentos de identidad como pasaportes o cédulas de identidad, la verificación de pasajeros en aeropuertos al embarcar y en aplicaciones y dispositivos de telefonía móvil (Wenger et al., 2023). Esa misma tecnología y sus derivaciones sirven de apoyo en estrategias de seguridad pública, pues permite la identificación de personas de interés, prófugos, personas desaparecidas o delincuentes (Cáceres y Guerra, 2024).

En general, las FRT funcionan a partir de un algoritmo que codifica automáticamente la imagen facial, al medir diversas características del rostro, y la compara con perfiles que están almacenados en el sistema o base de datos existente (Interpol, s/f). Esta imagen puede tener su origen en una foto, un video previo o ser captada en tiempo real. Por tanto, requiere de una recolección de imagen en dos momentos. En una primera ronda, esa imagen es captada y registrada; en una segunda, esa imagen es vuelta a captar y se compara con la plantilla inicial, a partir de la cual se produce la identificación (Cáceres y Guerra, 2024).

La imagen del rostro está compuesta por un número finito de elementos o características que varían en cada individuo y lo hacen único e identificable. Por lo anterior, se considera que, actualmente, el reconocimiento facial es un mecanismo de Inteligencia Artificial (IA)[3] de gran utilidad para preservar la seguridad pública, pues permite identificar a personas a distancia, incluso entre una gran multitud (Domingo, 2021:21). En este sentido, el reconocimiento facial realizado a través de un algoritmo automatizado se considera dentro de las técnicas de IA[4], en reemplazo de la labor de identificación y detección personal que normalmente llevan a cabo seres humanos (Rigano, 2019, citado en Domingo, 2021:21).

---

[2] Este capítulo contiene parte del informe BCN “El tratamiento de imágenes personales en espectáculos deportivos. Normativa en Chile y estudio de casos extranjeros” (2024), elaborado por Marcela Cáceres y Pedro Guerra.

[3] De acuerdo con Domingo (2021:21), “por Inteligencia Artificial se entiende la habilidad de una máquina para percibir y responder a su entorno de forma independiente y realizar tareas que normalmente requerirían de la inteligencia y de los procesos de toma de decisiones humanos, pero sin intervención directa de los mismos”.

[4] Una de estas técnicas es el “aprendizaje profundo” (*Deep learning*) se utiliza en procesos como el reconocimiento facial y del iris, donde los algoritmos reconocen bordes en un cierto nivel, la nariz en otro nivel y la cara en otro. Para lograrlo, el aprendizaje profundo requiere de macrodatos o datos masivos (*big data*) (Nalbandian, 2022).

Además, hoy las tecnologías de identificación permiten ir bastante más allá de la sola determinación de la identidad de una persona mediante la confrontación de una imagen con una plantilla. Las mediciones biométricas —esto es, utilizando datos biométricos— pueden ser de orden fisiológico, codificando ciertas características físicas individuales, tales como huella, forma de las manos, iris, forma de la cara o de las orejas, o pueden detectar un comportamiento humano, reconociendo la voz, la dinámica de la firma o la presión y velocidad de la pulsación en un teclado, que varían de persona a persona según su estado físico, edad o clase social (Quintanilla, 2020:68-69, en Cáceres y Guerra, 2024).

La FRT puede mejorar y acelerar las capacidades humanas existentes (como encontrar una persona individual en un video) o crear nuevas capacidades (como pretender detectar estados emocionales de personas en multitudes) (Lynch y Campbell, 2024).

Como señala la Agencia Europea de Derechos Fundamentales (*Fundamental Rights Agency, FRA*), la investigación en este ámbito ha permitido inferir otras características o estados personales de los sujetos que se someten a estas tecnologías, como orientación sexual, estados de ánimo o emociones, en procedimientos experimentales que son controversiales desde una perspectiva ética (FRA, 2019, en Cáceres y Guerra, 2024).

2. El uso de la tecnología de reconocimiento facial para el control de la inmigración

El informe "*Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe*", de la Universidad de Oxford (Ozkul, 2023:5-6), identifica y explora los diversos usos —algunos probados o implementados, pero luego cancelados— que actualmente permitirían la automatización de los procesos de inmigración, en diferentes países europeos. Entre otras funciones, estas tecnologías son utilizadas como herramientas para pronosticar la futura inmigración y desplazamiento hacia Europa; la tramitación de solicitudes de residencia y ciudadanía de corta y larga duración; la verificación de documentos de identidad; la evaluación y clasificación de riesgos en las solicitudes de viaje a la zona Schengen; la identificación y priorización de inmigrantes irregulares; la transliteración[5] de nombres y reconocimiento de dialectos con el fin de identificar el país de origen de los solicitantes de asilo; la distribución automatizada de beneficios sociales a solicitantes de asilo en Noruega; y el monitoreo electrónico de inmigrantes —para personas liberadas de la detención bajo fianza de inmigración con vulnerabilidades específicas— a través de dispositivos instalados, equipados con GPS (como tobilleras).

[5] Transliteración: método de representar los signos de un sistema de escritura mediante los signos de otro basándose en la similitud fonética (en la práctica, escribir una palabra usando un alfabeto diferente).

Respecto de estos últimos dispositivos, el Ministerio del Interior (*Home Office*) del Reino Unido ha planteado implementar relojes inteligentes basados en reconocimiento facial (dispositivos no instalados) (Ozkul, 2023:37). Estos requerirían a los inmigrantes que hubieren sido condenados por un delito penal escanear sus rostros hasta cinco veces al dia (Kelly, 2022). Sin embargo, hasta la fecha no han sido introducidos y no estarían contemplados en la actual política de libertad bajo fianza de inmigración (Home Office, 2024).

Para Wienroth y Amelung (2023), el reconocimiento facial automatizado, el uso de datos dactiloscópicos y los análisis forenses avanzados de ADN se están convirtiendo en los medios tecnológicos de vigilancia dominantes para el control de la llamada "crimigración". Para estos autores, la "crimigración" describiría la creciente criminalización de la migración, basada en una "crisis" percibida de migración masiva y su supuesto impacto negativo en la estabilidad y el bienestar nacional, materializándose en regímenes superpuestos de control de la delincuencia y la migración.

En este sentido, la "crimigración" describe la convergencia de esferas jurídicas previamente distintas de la delincuencia y el control migratorio en el contexto de una sospecha criminal generalizada hacia los migrantes (Aas, 2011; Stumpf, 2006, citados en Wienroth y Amelung, 2023). Además, la reducción progresiva de las rutas de migración legal conduciría a una criminalización activa de diversas formas de migración, (re) produciendo distinciones entre cruces fronterizos legales e ilegales (Wienroth y Amelung, 2023).

Por otra parte, si bien la tecnología de reconocimiento facial existe desde hace algún tiempo, la industria de la aviación ha comenzado a integrarla en los procesos existentes para la identificación de pasajeros. Junto con su potenciamiento gracias a la Inteligencia Artificial, la tecnologia de reconocimiento facial —y en general la biometría— se considera podría ayudar en la lucha contra pandemias globales al permitir procesos sin contacto, reduciendo así el riesgo de transmisión de enfermedades y aumentando el flujo de pasajeros a través de los puntos de control (Khan y Efthymiou, 2021).

Finalmente, aunque el uso de nuevas tecnologías tiene el potencial de facilitar algunos procesos de toma de decisiones, sus riesgos inherentes de sesgo, discriminación y posibles errores técnicos representan una amenaza significativa para los (potenciales) migrantes y solicitantes de asilo, quienes ya estarían privados de sus derechos y enfrentan desafíos en la búsqueda de soluciones jurídicas (Ozkul, 2023:5).

3. Los datos biométricos como datos personales

Como se ha señalado, las FRT se basan en la captación de una imagen facial sobre la cual se produce la comparación. Las imágenes faciales, según la Agencia Europea de Derechos Fundamentales, constituyen un dato biométrico que no se puede cambiar ni es fácil de ocultar, además de ser relativamente fácil de captar en comparación con otros datos

biométricos, como son las huellas digitales. Por lo tanto, un dato biométrico es un dato personal que resulta de un procesamiento tecnológico de alguna característica física, psicológica o de comportamiento de una persona natural, que permite confirmar de manera unívoca su identidad (FRA, 2019, en Cáceres y Guerra, 2024).

Dado que esta clase de información identifica o permite identificar a una persona, **constituye un dato personal**, pues detecta características biológicas o psicológicas. Santisteban apunta, entonces, que "las técnicas de reconocimiento facial suponen un tratamiento de datos personales" (Santisteban, 2021: 507, en Cáceres y Guerra, 2024). Esto, como se verá, es corroborado por las normas europeas sobre la materia y por las legislaciones nacionales que se han dictado. De la misma forma, el Consejo para la Transparencia, CPLT en Chile ha estimado en sus recomendaciones que la imagen del rostro de una persona puede "calificar en Chile de datos personales de carácter sensible (…) al corresponder a información que se refiere a las características físicas de una persona natural" (CPLT, 2021, en Cáceres y Guerra, 2024).

4. Reconocimiento facial y derechos fundamentales

Dado que esta tecnologías requieren recopilar datos personales, a partir del propósito de cada una de ellas es posible analizar el nivel de amenaza a los derechos fundamentales. En primer lugar, están aquéllas cuyo objetivo es la **verificación o autenticación** de una identidad personal. Así, por ejemplo, las cámaras que equipan algunos modelos de teléfonos celulares inteligentes tienen sistemas de verificación uno-a-uno (*one-to-one matching*), es decir, que comparan la imagen con una plantilla única —la propia imagen del dueño del equipo— y no requiere de un almacenamiento centralizado de la imagen (FRA, 2019, Cáceres y Guerra, 2024). Aquí el tratamiento del dato personal se adscribe a la persona específica que ha introducido su imagen en la plantilla y se consideraría en general como menos invasivo de la privacidad (Santisteban, 2021: 507, en Cáceres y Guerra, 2024).

En cambio, según la Agencia Europea de Derechos Fundamentales, en los sistemas de **identificación** uno-a-muchos (*one-to-many matching*), que comparan una imagen individual con las de muchas otras personas almacenadas en una base de datos, para determinar si esa imagen individual está contenida o almacenada en ella, podrían observarse mayores riesgos a los derechos fundamentales (FRA, 2019; Santiesteban, 2021; Pérez, 2022:81). Algunos de estos riesgos surgen del uso no autorizado de imágenes de terceros; otros, de la divulgación de esa información, y de los resultados de su procesamiento a terceros, ya sea organismos públicos, privados o personas naturales. Es precisamente ante estos riesgos que los sistemas jurídicos han elaborado respuestas más o menos desarrolladas y/o protectoras de los derechos individuales (Cáceres y Guerra, 2024).

a) Riesgos derivados de problemas técnicos

Los riesgos que se generan por problemas técnicos de las tecnologías aluden a que, si bien las tasas de error son menores[6], los sistemas son proclives a que ciertas categorías de personas sean identificadas erróneamente con más frecuencia que otras. Dado que las respuesta que proveen son binarias (se identifica o no) los mecanismos son susceptibles a producir falsos (positivos o negativos) en base a un cálculo probabilístico que el sistema procesa a alta velocidad. Como indica la Agencia Europea de Derechos Fundamentales, esto depende en buena parte de la calidad de la información con que se nutre la base de datos en la que el sistema busca una coincidencia facial. La calidad de las imágenes resulta fundamental, y ésta no siempre es óptima (Cáceres y Guerra, 2024).

Asimismo, como destaca la citada agencia europea, los *softwares* de reconocimiento facial se basan en modelos pre-entrenados que desarrollan reglas de identificación basadas en bases de datos con imágenes disponibles. En otras palabras, los sistemas son "enseñados" para desarrollar esa labor de identificación en base a la mayor o menor cantidad de información disponible y a un poder de computación dado y creciente. En estas condiciones, la falibilidad/fiabilidad del sistema descansa necesariamente en la calidad y la cantidad de información de que dispone para su labor; pero su entrenamiento en sí, es decir, la determinación de la forma en que operará, no está libre de sesgos (Cáceres y Guerra, 2024).

Como reporta la agencia (FRA, 2019), los sistemas de reconocimiento facial reportan problemas en identificación en género y grupos étnicos, ya que los *softwares* de reconocimiento facial son a menudo entrenados sobre imágenes faciales de hombres blancos y, en mucha menor medida, de mujeres y personas pertenecientes a otros grupos étnicos (Cáceres y Guerra, 2024). Investigaciones han demostrado que la inexactitud de identificación entre la población negra es mucho mayor que en otras comunidades raciales. Por su origen, la mayoría de los programas de software —de empresas como Microsoft, IBM y Megvii de China— reconocen a los caucásicos y asiáticos orientales con mayor precisión que otros grupos étnicos o raciales (por ej., mujeres de piel oscura) (Sarabdeen, 2022:1).

b) Riesgos desde la perspectiva jurídico-política

Como se evidencia en las discusiones de literatura, los dilemas radican en la mayor o menor afectación que las estrategias de seguridad basadas en el uso de la video vigilancia, y específicamente del reconocimiento facial automático, pueden generar para los derechos fundamentales. Ello a partir de la posición desmejorada o de debilidad de las personas

[6] La citada Agencia indica que el 0,01% de las identificaciones masivas en lugares como estaciones de trenes o aeropuertos serían erróneas. Ello implica, aun, que cientos de personas son erróneamente identificadas (FRA, 2020).

cuyos rostros son captados y chequeados por los sistemas de vigilancia (FRA, 2019, en Cáceres y Guerra, 2024).

Pérez (2022:61-62) identifica los problemas más gruesos de las FRT en torno al **derecho a la igualdad y la no discriminación**; a la **garantía de presunción de inocencia**; al **derecho a la privacidad** y a la **libertad ambulatoria**. El derecho a la privacidad, para Santisteban (2021:505), constituye un presupuesto para el ejercicio de otros derechos, como la libertad de expresión, pues este último reclama de cierto anonimato en el espacio público. Como se advierte, el espectro de derechos que pueden afectarse en el uso de tecnologías de esta clase es amplio, y dependerá de la robustez de las estructuras de protección existentes en cada país y de la rendicion de cuentas y responsabilidad (*accountability*) públicas de las instituciones privadas y del Estado. No es posible, en consecuencia, ofrecer un análisis exhaustivo, pues nuevas formas de afectación pueden aparecer en circunstancias específicas (Cáceres y Guerra, 2024).

No obstante, como se señalaba y siguiendo a la Agencia Europea de Derechos Fundamentales, hay un conjunto de derechos que debe tenerse en consideración en el desarrollo e implementación básicos de una regulación. El primer grupo lo componen el **respeto a la vida privada y la protección de los datos personales**. El derecho a la protección puede considerarse una extensión del primero, pero ambos emanan de la dignidad y la autonomía de la persona humana, que granjea una esfera personal en que se impide a otros la intromisión. El segundo grupo lo componen las **libertades de expresión, reunión y asociación** (Cáceres y Guerra, 2024).

II. Tendencia regulatoria internacional de protección de datos biométricos

Además de la instalación de esta tecnología en millones de teléfonos móviles para control de acceso del usuario, para el año 2019, los gobiernos de más de 64 países habrían implementado algún tipo de esquema de FRT (Kostka et al., 2023).

Regular el uso de la tecnología de reconocimiento facial presenta un dilema de Collingridge[7] con respecto a la gran demanda de principios legales comunes que permitan resolver los conflictos prácticos entre privacidad y eficiencia, autonomía y autoridad, y seguridad y responsabilidad (*accountability*) (Cheng y Wang, 2023).

Para Ozkul (2023:5), el uso de nuevas tecnologías también puede conducir a nuevas relaciones entre los sectores público y privado para desarrollar, sostener e implementar las mismas. Esto requiere nuevas estructuras de gobernanza y marcos legislativos que regulen

[7] El dilema clásico de Collingridge en los estudios de ciencia y tecnología consiste en que, si bien la tecnología puede controlarse en sus primeras etapas, no es posible saber lo suficiente sobre sus consecuencias dañinas sociales como para justificar el control de su desarrollo; pero, para cuando estas consecuencias son evidentes, el control se vuelve costoso y lento (Cheng y Wang, 2023).

quién se hace responsable de los riesgos de protección de datos y los posibles "errores técnicos" así como los resultados inexactos o discriminatorios relacionados a estos.

Ferreyra (2020, citado en Pérez, 2022:62) destaca que el sistema de reconocimiento debe contar con elementos de análisis, transparencia y control para poder evaluar apropiadamente la efectividad del reconocimiento facial; así como también debe estar dotado de la publicidad necesaria para que la ciudadanía sepa en dónde será captada por la tecnología. Por último, es también necesaria la protección de un órgano independiente para evitar excesos.

III. La normativa nacional aplicable al control migratorio por medio de datos biométricos[8]

En nuestro país, el principal texto legislativo sobre protección de datos personales en Chile es la Ley N° 19.628 sobre protección de la vida privada, que deriva de la garantia constitucional del artículo 19, N°4 de la Constitución Política de la República.

1. Regulación aplicable a los sistemas de reconocimiento facial

El artículo 2, letra f) de la Ley N° 19.628 define los datos de carácter personal como "(…) los relativos a cualquier información concerniente a personas naturales, identificadas o identificables". Una clase específica de datos personales son los datos sensibles, que define el mismo artículo en su letra g). Se trata de "(…) aquellos datos personales que se refieren a las **características físicas** o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual."

Por tanto, las imágenes de rostros de las personas son considerados como **dato personal sensible**, de acuerdo a la actual legislación. Este concepto debe entenderse de manera complementaria con la de tratamiento de datos, que se define en el artículo 2, letra o) como "(…) cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma."

De este modo, los sistemas de reconocimiento facial corresponderían a un sistema de tratamiento de datos. El artículo 4 de la Ley N°19.628, ordena que el tratamiento de datos

[8] Este capítulo contiene parte del informe BCN "El tratamiento de imágenes personales en espectáculos deportivos. Normativa en Chile y estudio de casos extranjeros" (2024), de Marcela Cáceres y Pedro Guerra.

sólo puede efectuarse cuando la ley u otras disposiciones legales lo autoricen; o bien cuando el titular de los derechos consienta expresamente en ese tratamiento. Teniendo en cuenta esas restricciones, y la regulación detallada que la ley hace de la forma de otorgar ese consentimiento[9], es preciso determinar si la ley chilena autorizaría el tratamiento de imágenes personales que hayan sido captadas por sistema de reconocimiento facial.

La primera consideración que debe hacerse es que, como señala el Consejo para la Transparencia (CPLT), la tecnología de reconocimiento facial no posee una regulación expresa en la legislación (CPLT, 2021:69). Eso hace aplicable el régimen general de la Ley N° 19.628, en su acápite de datos personales. Entonces, una entidad que opere en Chile un sistema de videovigilancia o de reconocimiento facial, está obligada a cumplir con las normas de esta ley.

Estas obligaciones legales le incumben a cualquier persona natural o jurídica que opere el sistema en calidad de responsable de banco de datos, ya sean instituciones públicas o privadas. En ese sentido, para el CPLT es claro que el funcionamiento de los sistemas de videovigilancia y captación de imágenes implica necesariamente el tratamiento de datos personales en los términos en los que lo define la ley e independientemente del nivel de cada operación (CPLT, 2021:72). Esto incluye, en cualquier caso "(…) el match realizado entre los datos captados mediante cámaras con una base de datos que contenga datos biométricos o huellas faciales y que fueron almacenados con anterioridad." (CPLT, 2021:72).

Asimismo, el alcance de la regulación actual para el problema del tratamiento de imágenes faciales es amplio, y comprende tanto las imágenes que se obtienen del rostro de una persona, como aquellas que ya se encuentran almacenadas en otras bases y que van a servir para la comparación e identificación de una persona. Estas últimas suelen denominarse "*watch list*" o lista de vigilancia, y se compilan por las policías y fuerzas de seguridad, para después ser sometidas al cotejo digital.

La aplicación del régimen de la Ley Nº 19.628 a los datos personales sensibles que constituyen las imágenes faciales impone al tratamiento de dichas imágenes algunos requisitos. Debe, en primer lugar, estar expresamente contenido en una ley; en caso de no estarlo, debe resultar imprescindible para el debido cumplimiento de una función pública establecida por ley, en caso de que el tratamiento corresponda a organismos públicos en ejercicio de una función que les es propia (art. 20, Ley Nº 19.628). En segundo lugar, debe haber sido obtenida con el consentimiento del titular, expreso, por escrito y previa información a éste.

[9] Según el mismo artículo 4, el consentimiento debe otorgarse por escrito y previa información al titular. La excepción al consentimiento es el caso de datos que provienen de fuentes accesibles al público.

Como se advierte, la base de legalidad para el tratamiento de las imágenes personales o faciales captadas por sistemas de reconocimiento es, en la actualidad, la ley o el consentimiento del titular. Por lo tanto, si se tratara de captar imágenes faciales de personas en forma masiva o indiscriminada, estas no contarían con un respaldo de legalidad en la actual normativa que rige en Chile, y su tratamiento no estaría autorizado por la ley. Ello, salvo que las personas que son captadas otorguen su consentimiento, en los términos que dispone la Ley Nº 19.628.

2. Proyecto de ley sobre protección de datos personales

Actualmente se encuentra en tercer trámite constitucional, en el Senado, el proyecto de ley de protección de datos personales que reforma la Ley N° 19.628[10]. Este proyecto obedece en buena parte a las críticas que ha recibido el actual sistema de protección de datos personales. En ese sentido, el Consejo para la Transparencia ha señalado que la actual legislación resulta insuficiente para el objetivo de protección.

Entre otras críticas, el CPLT destaca que los principios de tratamiento de los datos están regulados de forma inorgánica y deficiente, que las bases de legalidad son limitadas, pues de basan únicamente en la ley y el consentimiento del titular, y que no se contemplan regulaciones sobre categorías de datos relevantes, como los datos biométricos y de geolocalización. El corolario es que no existe "un mayor control respecto de la implementación en Chile de tecnologías de videovigilancia y reconocimiento facial, por ejemplo, en contextos de seguridad de espacios públicos." (CPLT, 2021:85–86).

En ese orden, el proyecto de ley innova en los siguientes aspectos relativos a la protección de esta clase de datos:

a) Definición de dato personal:

El proyecto contempla definirlos como "(…) cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, el análisis de **elementos propios de la identidad física, fisiológica, genética, psíquica**, económica, cultural o social de dicha persona, excluyendo aquellos casos en que el esfuerzo de identificación sea desproporcionado."

[10] Proyecto de ley que regula la protección y el tratamiento de datos personales y crea la Agencia de Protección de Datos Personales (Boletín 11.092-07 y 11.144-07, refundidos).

b) Definición datos personales sensibles:

La modificación propuesta, actualmente en discusión, es la siguiente: "(…) sólo tendrán esta condición aquellos datos personales que revelen el origen étnico o racial, la afiliación política, sindical o gremial, hábitos personales, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los **datos biométricos**, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural."

c) Definición de dato biométrico:

El proyecto de ley, a diferencia de la ley actual, sí ofrece un concepto de dato biométrico, como "(…) aquellos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación única de ella, tales como la huella digital, el iris, los rasgos de la mano o **faciales** y la voz."

Como se advierte, las definiciones que propone el proyecto de ley permiten incorporar categorías más amplias de lo puede entenderse como dato personal sensible, en los que queda claramente incorporado. Esto se debe comprender como parte de un conjunto de definiciones que componen el sistema de protección, como la de "elaboración de perfiles" (formas de tratamiento automatizado de datos personales para análisis o predicción) o "tratamiento de datos" (cualquier operación o procedimientos técnicos, que permitan utilizar de cualquier forma datos o conjuntos de datos personales).

En un mismo sentido, una de las innovaciones del proyecto en relación a la actual ley es el establecimiento de principios que gobiernan el uso protegido de los datos. Entre los más relevantes, y que inciden directamente en la cuestión de la identificación facial por sistemas de televigilancia, están el principio de licitud, que implica que los datos personales sólo pueden tratarse con sujeción a la ley; y el de finalidad, que exige que los datos sean recolectados con fines específicos, explícitos y lícitos, y que su tratamiento esté limitado a esos fines.

3. Registro biométrico para personas con ingreso irregular al país

En Chile, por Resolución 25.425 Exenta, de 2023, del Servicio Nacional de Migraciones, se estableció un procedimiento para el registro o empadronamiento biométrico de personas extranjeras que hayan ingresado al país por paso no habilitado, que se efectuó de forma presencial entre el 27 de junio de 2023 hasta el 31 de diciembre de 2023, en las dependencias de la Policía de Investigaciones de Chile.

Entre sus fundamentos, se señala que el Servicio Nacional de Migraciones es el organismo público encargado de establecer, organizar y mantener el Registro Nacional de Extranjeros

(art. 157 N°11, Ley N°21.325 de Migración y Extranjería), el cual debe contener entre otros asuntos, la identificación de los extranjeros que se encuentren en el país y el domicilio de los residentes. Asimismo, corresponde a la Policía de Investigaciones de Chile controlar el ingreso y la salida de personas del territorio nacional, adoptar todas las medidas conducentes para asegurar la correcta identificación de quienes salen e ingresan al país, verificar la validez y autenticidad de sus documentos de viaje y fiscalizar la permanencia de extranjeros en el país.

De acuerdo a la Resolución, el empadronamiento biométrico de las personas extranjeras se realizará a quienes cumplan los siguientes requisitos copulativos:

a) Ser mayor de 18 años,
b) Haber ingresado a Chile por paso no habilitado o eludiendo el control migratorio correspondiente en frontera, hasta el día 30 de mayo de 2023 (extendido posteriormente hasta fines de 2023),
c) Que registren Informe Policial que denuncia su ingreso al país por pasos no habilitados o eludiendo el control migratorio; o que hayan realizado la Declaración Voluntaria de Ingreso por paso no habilitado ante la Policía de Investigaciones de Chile; y
d) Que se encuentren actualmente en Chile.

Ante la PDI, la persona extranjera debía presentar el documento de identidad o pasaporte (vigente o vencido) para su verificación y registro, procediendo a la captura de fotografía y toma de huellas dactilares. De acuerdo al Servicio Nacional de Migraciones, Luis Eduardo Thayer, a septiembre de 2023, gracias a la buena convocatoria de la iniciativa, más de 70 mil personas ya se encontraban empadronadas en todo el país (Servicio Nacional de Migraciones, 2023).

Dicho empadronamiento biometrico, si bien constituiría un caso de tratamiento de datos personales sensibles, de acuerdo a la Ley Nº 19.628, no estaría expresamente contenido en una ley (lo esta en una norma de rango inferior, como es una resolución exenta). Por tanto, necesariamente debe cumplir con el requsito de ser imprescindible para el debido cumplimiento de una función pública establecida por ley, por tratarse de un organismo público (el Servicio Nacional de Migraciones) en ejercicio de una función que le es propia.

Por otra parte, se destaca que este registro no constituye un caso de aplicación de una tecnología de reconocimiento facial, sino que crea una base de datos (que contendria las plantillas) que posteriormente podría servir para el uso de FRT en controles migratorios.

IV. Experiencias extranjeras que utilizan el control biométrico para el control migratorio

En EE. UU. y otros países desarrollados, los sistemas de reconocimiento facial y análisis de expresiones faciales comenzaron a desarrollarse en las décadas de 1960 y 1970, en laboratorios de investigación financiados por el Ministerio de Defensa norteamericano y los servicios de inteligencia. En 1990 se crearon nuevas empresas para comercializar la tecnología, que buscaban mercados objetivo, en particular, entre las instituciones que utilizaban sus propias redes informáticas, como la industria financiera, las empresas, los sistemas de identificación a gran escala, los servicios de pasaportes, los organismos públicos, las fuerzas de orden y los sistemas penitenciarios (Utegen y Rakhmetov, 2023:829).

En ausencia de legislación, muchas jurisdicciones en todo el mundo han establecido principios y directrices a nivel estatal para regular algoritmos y tecnologías basadas en datos, como FRT. Aunque los principios y orientaciones de este tipo son útiles para establecer expectativas de alto nivel y afianzar valores fundamentales, carecen de cualquier mecanismos para exigir su cumplimiento (Lynch y Campbell, 2024).

1. Australia y Nueva Zelanda

Según Lynch y Campbell (2024), Australia y Nueva Zelanda han experimentado un crecimiento significativo en el uso de FRT por parte del Estado y/o del sector público —gobierno, policía y seguridad— pero la regulación sigue siendo irregular.

a) La recolección de datos y administración de los sistemas biométricos

El sistema de autoservicio tipo quiosco llamado eGate, operado por el Servicio de Aduanas de Nueva Zelanda, permite controlar pasaportes en forma automatizada por medio del uso de tecnología de reconocimiento facial. Está disponible en cuatro aeropuertos de Nueva Zelanda para viajeros que llegan y salen del país (New Zealand Customs Service, 2024).

Aunque es voluntario, solo pueden utilizar eGate las personas mayores de 12 años que cuenten con un pasaporte electrónico de determinados países. Este sistema utiliza datos biométricos para hacer coincidir la imagen del rostro del pasajero contenida en su pasaporte electrónico (*ePassport*) con la fotografía que se le toma en la puerta de embarque/desembarque (New Zealand Customs Service, 2024).

El mismo sistema, denominado SmartGates, implementado en 2007, es operado por la Fuerza Fronteriza de Australia, y está ubicado en los puntos de control de inmigración en las salas de salidas y llegadas en diez aeropuertos internacionales australianos. A diferencia del caso neozelandés, solo pueden utilizar el sistema las personas mayores de 16 años, o de entre 10 y 15 años, si se trata de un ciudadano australiano acompañado por al menos 2 adultos (Australian Border Force, 2019).

Desde 2019, el gobierno australiano ha empujado la mejora de SmartGates, el que habría sufrido retrocesos por razones tecnológicas y de la pandemia. Como parte de la iniciativa más amplia llamada "*Seamless Traveller*" —desarrollada como un proceso migratorio sin contacto—, el nuevo sistema a implementar a partir de 2022 es un "sistema de dos etapas", muy parecido a la configuración existente. Este, desarrollado por la empresa IDEMIA, requiere que los pasajeros se procesen en un quiosco SmartGate —para confirmar y validar su identidad— y luego en una unidad de puerta de embarque/desembarque, donde utilizarán su rostro en vivo como *token* para su identificación. La "validación biométrica" se realizará en ambas etapas del viaje (Hendry, 2022).

Por tanto, se diferencia de una propuesta de 2017 (realizada por otra empresa), que pretendía utilizar puertas de embarque/desembarque habilitadas para reconocimiento facial, que comparían los rostros de los viajeros con imágenes faciales almacenadas en los sistemas avanzados de procesamiento de pasajeros de las aerolíneas, sin exigirles que presentaran un pasaporte o utilizaran un un quiosco (Hendry, 2022).

b) La regulación de la tecnología de reconocimiento facial

Uno de los principales usos de FRT está establecido en la seguridad fronteriza y el control de la inmigración de ambos países, a través del sistema SmartGate. La autorización electrónica de viaje a Australia (*Australian Electronic Travel Authority,* ETA) actualmente puede obtenerse mediante una aplicación, utilizando FRT. Este es un caso de uso de "verificación" (uno-a-uno), pero en este ámbito también exisitirían evidentes casos de uso de "identificación" (uno-a-muchos).

La agencia de inmigración neozelandesa confirma la identidad de una persona comparando una fotografía o una huella digital con una versión almacenada, siendo el reconocimiento facial mediante la fotografía el uso más común de la información biométrica. Asimismo, indica en su sitio web que, en determinadas circunstancias podría utilizar muestras de ADN (New Zealand Immigration, s/f).

La Ley de Inmigración de Nueva Zelanda (*Immigration Act 2009*) permite a Inmigración de Nueva Zelanda (INZ) recopilar información biométrica. La sección 30 dispone que la información biométrica (incluidas las imágenes faciales) requerida a las personas de conformidad con esta ley, puede usarse para establecer un registro de identidad de un individuo, para establecer o verificar la identidad de alguien en particular o para ayudar en la toma de decisiones.

De este modo, señala INZ, se recopilan fotografías y huellas dactilares para:

- Identificar y comprobar la identidad de los extranjeros que buscan reasentamiento.
- Ayudar a identificar a los refugiados bajo el programa de cuotas de Nueva Zelanda.
- Identificar y controlar a personas bajo investigación en la frontera.
- Registrar la identidad de personas deportadas y evitar que vuelvan a ingresar a Nueva Zelanda con otra identidad.
- Identificar y controlar a personas sospechosas de infringir la ley.
- Exponer identidades supuestas.

En este sentido, la detección de fraude de identidad es el principal caso de uso (Lynch y Campbell, 2024), sea para evitar el ocultamiento de antecedentes penales o la reclamación falsa de la condición de refugiado (New Zealand Immigration, s/f).

La citada ley exige al INZ la recopilación de la información biométrica del solicitante de visa. La negativa puede resultar en el rechazo de la solicitud. En el caso de los ciudadanos neozelandes, estos proporcionan su identidad facial a través de sus pasaportes, pero el INZ no recopila sus huellas dactilares (New Zealand Immigration, s/f).

Por otra parte, de acuerdo a un informe del Ministerio de Empresa, Innovación y Empleo de 2016, Nueva Zelanda recibe y envía a los miembros de la Conferencia de los Cinco Países (FCC)[11] información biométrica (rostro y huellas dactilares), biográfica y criminalística sobre ciudadanos extranjeros expulsados de las fronteras de la FCC que hayan cometido delitos penales graves (Ministry of Business, Innovation and Employment, 2016:109).

La información biométrica es información personal y está regulada por la Ley de Privacidad de 2020 (*Privacy Act 2020*), que regula las obligaciones sobre seguridad, exactitud, retención, uso y divulgación de información personal —incluyendo la información biométrica— y consagra los derechos de acceso y solicitud de corrección de la información (Privacy Commissioner, 2021).

[11] La FCC es un acuerdo internacional para intercambiar información en materia de inmigración. Sus miembros son: Nueva Zelanda, Australia, Reino Unido, Canadá y Estados Unidos (New Zealand Immigration, s/f).

Sin embargo, no existe un set de reglas específicas para los datos biométricos. Por tanto, se encuentra en discusión una propuesta de la Oficina del Comisionado de Privacidad para la creación de un código de buenas prácticas bajo el marco de la Ley de Privacidad 2020 (Privacy Commissioner, s/f).

El borrador del *Biometric Processing Privacy Code* estará disponible para comentarios hasta el 8 de mayo de 2024, en relación a las siguientes (Privacy Commissioner, s/f):

1) ¿Debieran las agencias (públicas o privadas) demostrar que los argumentos a favor superan los argumentos en contra respecto de los biométricos antes de usarlos? (proporcionalidad). ¿Debieran las agencias adoptar salvaguardias razonables y relevantes, como pedir el consentimiento cuando sea apropiado, probar el sistema y monitorear resultados defectuosos?
2) ¿Debieran las personas ser informadas clara y obviamente cuando sus biométricos son recolectados? (transparencia). ¿Debieran usar señales y noticias en inglés simple y decir públicamente por cuanto tiempo guardarán la información biométrica?
3) ¿Cuáles son algunas cosas para las cuales los biométricos nunca debieran ser usados? (limitaciones). ¿Está de acuerdo con que esas cosas puedan ser utlizados: detectar información de salud, asumir emociones y predecir género, edad o etnia?

2. Unión Europea

El uso gubernamental de la FRT en la Unión Europea (UE) se encontraría limitado hasta el momento. Austria, Finlandia, Francia, Alemania, Grecia, Hungría, Italia, Letonia, Lituania, Eslovenia y los Países Bajos ya la estarían implementando de manera experimental y localizadas. En particular, la tecnología sería usada principalmente por las autoridades de los paises europeos con fines de prevención, investigación, detección y enjuiciamiento de delitos penales, así como para la prevención de amenazas a la seguridad pública (Kuhlmann, 2024).

Asimismo, su uso estaría aumentando gradualmente en los ámbitos de la migración y el asilo en toda Europa. Varios estados han comenzado a usarlos (o probarlos) para controlar quién ingresa a sus fronteras o para elegir quién obtiene acceso a sus territorios o sus mecanismos de protección (Ozkul, 2023).

a) La recolección de datos y administración de los sistemas biométricos

En 2020, la Agencia de la Unión Europea para la Gestión Operativa de Sistemas TI de Gran Escala en el Espacio de Libertad, Seguridad y Justicia (eu-LISA)[12], firmó un contrato marco

[12] eu-LISA es una agencia de la Unión Europea creada en 2011 para proporcionar una solución a largo plazo para la gestión operativa de sistemas informáticos a gran escala, que son instrumentos esenciales en la implementación de las políticas de asilo, gestión de fronteras y migración de la UE (eu-LISA, s/f-a).

para un nuevo sistema de comparación biométrica que tiene como objetivo crear una base de datos de huellas dactilares e imágenes faciales de más de 400 millones de nacionales de "terceros países" para 2024. Este emergente Sistema de Comparación Biométrica (sBMS) está destinado a abordar la "migración ilegal" y la delincuencia transfronteriza en los 26 países europeos del área Schengen sin pasaporte, convirtiéndolo en uno de los sistemas biométricos más grandes del mundo (Wienroth y Amelung, 2023).

El sBMS representa esfuerzos para integrar diferentes tecnologías biométricas y bases de datos, incluidos Eurodac[13], el Sistema de Información de Visas (VIS, por sus siglas en inglés) y el Sistema de Información de Schengen (SIS) (Wienroth y Amelung, 2023; eu-LISA, s/f-a).

Además de los anteriores, eu-LISA está desarrollando el Sistema de Entrada/Salida (EES, por sus siglas en inglés), el Sistema Europeo de Información y Autorización de Viajes (ETIAS, por sus siglas en inglés) y el Sistema Europeo de Información de Antecedentes Penales-Nacionales de Terceros Países (ECRIS-TCN, por sus siglas en inglés) (eu-LISA, s/f-a).

b) La regulación de la tecnología de reconocimiento facial

Si bien se encuentran vigentes normas europeas de protección de datos personales, tales como el Reglamento General de Protección de Datos[14] (GDPR, por sus siglas en inglés) y la Directiva (UE) 2016/680[15], de protección de datos personales en el marco de la prevención y detección de infracciones penales[16], hasta el momento no existe legislación que aborde el uso de FRT (Kuhlmann, 2024), y menos aún específicamenmte en el ámbito del control de la inmigración.

Sin embargo, existen orientaciones sobre la materia a nivel europeo. De acuerdo a las Directrices sobre tecnología de reconocimiento facial en el ámbito de la aplicación de la ley

---

[13] Eurodac es un sistema informático a gran escala que ayuda a la gestión de solicitudes de asilo europeas desde 2003, almacenando y procesando las huellas dactilares digitalizadas de solicitantes de asilo e inmigrantes irregulares que han entrado en un país europeo. De esta manera, el sistema ayuda a identificar nuevas solicitudes de asilo frente a las ya registradas en la base de datos (eu-LISA, s/f-b).

[14] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

[15] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

[16] Mientras la Directiva citada regula la protección de las personas naturales en cuanto al tratamiento de sus datos personales por parte de las autoridades competentes en el ámbito penal (art. 1.1, LED), el GDPR establece regula la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y la libre circulación de los mismos (art. 1.1, GDPR).

(*Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*), adoptadas por el Comité Europeo de Protección de Datos (CEPD)[17] en 2023, el uso de FRT está intrínsecamente vinculado al procesamiento de cantidades significativas de datos personales. Estas directrices proporcionan orientación a los legisladores nacionales y de la UE, así como a las autoridades encargadas de hacer cumplir la ley, sobre la implementación y el uso de este tipo de sistemas (EDPB, 2023-b).

Las citadas directrices concluyen que el rostro y, en general, los datos biométricos, estarían vinculados permanente e irrevocablemente a la identidad de una persona. Por ello, el uso del reconocimiento facial impactaría una serie de derechos y libertades consagrados en la Carta de Derechos Fundamentales de la UE. Entre estos no solo se encontrarían la privacidad y la protección de datos, sino también la dignidad humana, la libertad de movimiento, la libertad de reunión, entre otros, lo que sería particularmente relevante en el área de aplicación de la ley (tales como investigaciones y justicia penal) (EDPB, 2023-a).

Entre otras recomendaciones, las directrices subrayan que las herramientas de reconocimiento facial sólo deben utilizarse en estricto cumplimiento de la Directiva (UE) 2016/680. Además, tales herramientas sólo deben utilizarse si son necesarias, proporcionadas y apropiadas para alcanzar los legítimos objetivos legislativos, tal como lo exige la Carta de los Derechos Fundamentales de la UE. En las directrices, el CEPD reitera su petición de prohibir el uso de la tecnología de reconocimiento facial en determinados casos, como había solicitado anteriormente en el dictamen conjunto CEPD-SEPD sobre la propuesta de Ley sobre Inteligencia Artificial[18] (EDPB, 2023-a).

Finalmente, las directrices señalan que ciertos casos de uso de FRT, como la identificación biométrica remota de personas en espacios de acceso público (equivalente a una vigilancia masiva), plantean riesgos inaceptablemente altos para los individuos y la sociedad. Por estos motivos, el CEPD y el SEPD han pedido su prohibición general. En la misma línea, el CEPD considera que los sistemas de reconocimiento facial basados en inteligencia artificial, que clasifican a las personas en función de sus datos biométricos en grupos según su origen étnico, género y orientación política o sexual, no son compatibles con la Carta (EDPB, 2023-b). Por tanto, si bien las directrices no señalan específicamente la inmigración como uno de sus ámbitos específicos de aplicación, estas recomendaciones serían relevantes para las agencias encargadas del cumplimiento de la legislación migratoria.

---

[17] El Comité Europeo de Protección de Datos (CEPD) es un organismo europeo independiente que coordina y reúne a las autoridades nacionales de protección de datos de los países del Espacio Económico Europeo, así como a la autoridad europeo de protección de datos (SEPD) (EDPB, s/f).

[18] La Ley de Inteligencia Artificial (Ley de IA) es una normativa en desarrollo de la Unión Europea —casi finalizada— que introducirá un marco regulatorio y legal común para la IA en todos los sectores (excluido el militar) y todos los tipos de IA. Contiene una presunción que prohíbe los sistemas de IA de alto riesgo a menos que su uso esté sujeto a diversos requisitos, incluido un procedimiento de control y monitoreo, además del deber de informar incidentes y mal funcionamiento graves (Lynch y Campbell, 2024).

3. Estados Unidos

De acuerdo con Nalbandian (2023), Estados Unidos gestiona la migración mediante la recopilación y el uso de múltiples datos, obtenidos de una variedad de fuentes, incluyendo información proveniente de registros oficiales (de antecedentes criminales, vehículos motorizados, bienes raíces, licencias de conducir, judiciales, tributarios y servicios públicos), bases de datos comerciales (seguros, bancos, proveedores de atención médica, historial crediticio) e incluso de escaneos, tatuajes y redes sociales. A estos se suman algunos de carácter personalísimo, como son los datos biográficos y biométricos, incluidas huellas dactilares, huellas palmares, imágenes faciales y escaneos del iris, ADN, y reconocimiento de voz.

a) La recolección de datos y administración de los sistemas biométricos

La práctica de utilizar cámaras de vigilancia para reconocimiento facial se inició en el contexto de las medidas antiterroristas adoptadas después del 11 de septiembre de 2001. Basado en la Ley de Seguridad Fronteriza (*Enhanced Border Security and Visa Entry Reform Act of 2002*), se introdujeron los documentos de identidad biométricos y el uso de identificadores biométricos en las visas (Utegen y Rakhmetov, 2023:828; Travel.State.Gov (2024).

Desde 2004, las agencias y departamentos federales utilizan la tecnología de reconocimiento facial principalmente para acceso digital, aplicación/cumplimiento de la ley y seguridad física, para lo cual el gobierno crea sus propias bases de datos y utiliza software comercial —y sus bases de datos— para realizar búsquedas (Sarabdeen, 2022:3).

En particular, la agencia de Aduanas y Protección de Fronteras de los EE.UU. (*U.S. Customs and Border Protection*, CBP) ha implementado con éxito la biometría facial (llamada *Traveler Verification Service,* TVS) en los procesos de entrada en todos los aeropuertos internacionales —conocido como Llegada Simplificada (*Simplified Arrival*)—, y en los procesos de salida en 49 aeropuertos. CBP también amplió la biometría facial en 39 puertos marítimos y todos los carriles peatonales en los puertos de entrada de la frontera suroeste y norte (CBP, 2024).

Con la progresiva eliminación de los quioscos de “control automatizado de pasaportes” que debutaron en 2013, desde el año 2018 la CBP usa cada vez más el sistema de Llegada Simplificada. Este utiliza cámaras ubicadas junto a los funcionarios de inmigración para tomar una fotografía cuando un viajero se acerca y la compara con una fotografía de pasaporte o visa existente en el archivo. La agencia también ha implementado un programa de salida biométrico que escanea los rostros de los pasajeros que salen del país en tres docenas de aeropuertos (Iyengar y Gutman-Argemí, 2023).

La verificación de datos biométricos en bases de datos gubernamentales tiene como objetivo el identificar a personas sospechosas de terrorismo, criminales buscados o infractores de la legislación de inmigración de los EE.UU. (Utegen y Rakhmetov, 2023:828).

En febrero de 2018, una empresa privada (Northrop Grumman) celebró un contrato con el gobierno norteamericano para desarrollar la nueva base de datos biométrica del Departamento de Seguridad Nacional (*Department of Homeland Security*, DHS), llamada Tecnología de Reconocimiento Avanzado Nacional (HART, por sus siglas en inglés) (Nalbandian, 2023).

El predecesor de HART, el Sistema Automatizado de Identificación Biométrica (IDENT, por sus siglas en inglés), almacenaba datos biográficos y biométricos, incluidas huellas dactilares, huellas palmares, imágenes faciales y escaneos del iris, y otras informaciones, de delincuentes sexuales, prófugos, deportados, infractores de normas de inmigración e individuos con antecedentes penales (Nalbandian, 2023).

El sistema HART tiene capacidad para almacenar al menos 500 millones de identidades únicas, incluidos los datos biométricos, y el ADN, reconocimiento facial y de voz, escaneos, tatuajes y "otras modalidades". Al igual que su predecesor, HART —y su *big data*—se alojará en GovCloud de Amazon Web Services (AWS) (Nalbandian, 2023).

Sin embargo, múltiples casos de identificaciones erróneas en las últimas décadas —especialmente de personas de raza negra— por parte de las fuerzas de orden, llevaron a la sociedad civil estadounidense y a organizaciones no gubernamentales internacionales a llamar a una prohibición masiva de las tecnologías de reconocimiento biométrico que permitieran una vigilancia masiva y discriminatoria (Utegen y Rakhmetov, 2023:830).

Es de notar que un informe de *Government Accountability Office* (GAO) [Oficina de Rendición de Cuentas del Gobierno de los EE.UU.], de marzo de 2024, descubrió que, en siete agencias[19] de los Departamentos de Seguridad Nacional y Justicia que habían informado utilizar la tecnología de reconocimiento facial para respaldar investigaciones criminales (entre las que se encuentra *U.S. Customs and Border Protection*), ninguna requirió que el personal recibiera la correspondiente capacitación (U.S. GAO, 2024).

b) La regulación de la tecnología de reconocimiento facial

De acuerdo con un informe de 2024 de las Academias Nacionales de Ciencias, Ingeniería y Medicina (*National Academies of Sciences, Engineering, and Medicine*), solicitado por el Departamento de *Homeland Security,* salvo algunas excepciones, EE.UU. no cuenta con guías, regulaciones o leyes que aborden adecuadamente los problemas relacionados con el uso de la tecnología de reconocimiento facial (National Academies of Sciences, Engineering, and Medicine, 2024).

[19] Las agencias son Aduanas y Protección Fronteriza de EE.UU. (*U.S. Customs and Border Protection*), el Buró Federal de Investigaciones (FBI, por sus siglas en inglés), el Servicio Secreto de los EE.UU., el Buró de Alcohol, Tabaco, Armas de Fuego y Explosivos, la Administración para el Control de Drogas (DEA, por sus siglas en inglés), Investigaciones de Seguridad Nacional y el Servicio de Alguaciles de los EE.UU. (U.S. GAO, 2024).

Si bien el informe reconoce el valor de la tecnología de reconocimiento facial[20] y no aboga por una prohibición general, señala que varios usos podrían causar suficiente preocupación como para prohibirlos. Por lo tanto, recomienda que se dicte una legislación federal y una orden ejecutiva con pautas para el uso adecuado de la tecnología por parte de los departamentos y agencias federales, así como se preste atención al tema por parte de los tribunales, el sector privado, las organizaciones de la sociedad civil y otras organizaciones que trabajan con ella (National Academies of Sciences, Engineering, and Medicine, 2024).

De acuerdo con el mismo informe, una nueva legislación federal debiera abordar las preocupaciones sobre equidad, privacidad y libertades civiles; limitar los posibles daños a los derechos individuales por parte de actores públicos y privados; y proteger contra el mal uso de la tecnología de reconocimiento facial. Específicamente, los legisladores deberían considerar:

- Establecer limitaciones al almacenamiento de imágenes faciales y plantillas.
- Requerir capacitación y certificación de operadores de sistemas y tomadores de decisiones, especialmente para aplicaciones donde los errores pueden dañar significativamente a los sujetos, como la accion policial.
- Abordar preocupaciones específicas de uso —por ejemplo, para vigilancia masiva o individual, acoso o chantaje, acceso a la vivienda y otros usos públicos y privados— que podrían inhibir intencionalmente o de otro modo el ejercicio de las libertades políticas y civiles.
- Promulgar una ley federal de privacidad específica para la tecnología de reconocimiento facial, o una legislación de privacidad más amplia que aborde prácticas comerciales que comprometan la privacidad.

Se destaca que en 2023 se introdujeron en el Congreso de los EE.UU. diversos proyectos de ley sobre la materia. Dos[21] de ellos imponen límites al uso de sistemas de vigilancia biométrica —incluyendo aquellos de reconocimiento facial— por parte de entidades gubernamentales federales, estatales y locales[22]. El proyecto define el término "reconocimiento facial" como un proceso automatizado o semiautomático que:

Ayuda a identificar a un individuo, capturar información sobre un individuo o generar o ayudar a generar información de vigilancia sobre un individuo en función de las características físicas de su rostro; o

---

[20] No se revisan aquí casos de "reconocimiento facial no dirigido" (*untargeted face recognition*), esto es, un sistema que identifica, no a personas particulares, sino a todos los individuos presentes en una transmisión de video (por ejemplo, para identificar a inmigrantes irregulares fuera de colegios u hospitales).

[21] *S.681 - Facial Recognition and Biometric Technology Moratorium Act of 2023.*

[22] Este proyecto de ley, presentado en el Senado, tiene el mismo nombre que otro presentado en la Cámara de Representantes (*H.R.1404 - Facial Recognition and Biometric Technology Moratorium Act of 2023*).

Registra las características de la cara, la cabeza o el cuerpo de un individuo para inferir emociones, asociaciones, actividades o la ubicación de un individuo.

Otro proyecto de ley[23] contiene una lista de restricciones a la aplicación de la tecnología de reconocimiento facial para hacer cumplir las leyes de inmigración. Por su parte, los organismos encargados de hacer cumplir la ley deben probar el sistema de reconocimiento facial y presentar informes anuales sobre la eficiencia de su implementación. Uno de los criterios importantes es eliminar de las bases de datos las imágenes de menores absueltos o puestos en libertad sin cargos.

Finalmente, se destaca la existencia de regulaciones municipales y estaduales en materia de reconocimiento facial. Entre las excepciones mencionadas previamente se encuentra la ciudad de San Francisco, en California. En 2019, ésta aprobó la primera ordenanza del país en prohibir a la policía y otras agencias gubernamentales el uso de tecnología de reconocimiento facial (Utegen y Rakhmetov, 2023:830). La "Ordenanza sobre Adquisición de Tecnología de Vigilancia"[24] prohíbe el uso de esta tecnología, con excepciones limitadas[25], y exige la publicación de las tecnologías de vigilancia actuales en posesión o uso de los departamentos de la ciudad. La ordenanza también requiere que el Comité de Tecnología de la Información colabore en el desarrollo, revisión y aprobación de las correspondientes políticas, antes de enviar sus recomendaciones al concejo municipal (San Francisco Police Department, 2024).

Aunque la mayoría de los estados iniciaron la introducción y regulación de la tecnología de reconocimiento facial para fines comerciales[26], California fue el primer estado, en 2019, en prohibir el uso de la tecnología de reconocimiento facial por parte de las autoridades. Posteriormente, esta práctica habría influido en la prohibición del uso de la tecnología de reconocimiento facial no solo por parte de las autoridades, sino también de las organizaciones privadas (Utegen y Rakhmetov, 2023:830).

---

[23] *H.R.6092 - Facial Recognition Act of 2023.*

[24] Esta ordenanza se encuentra contenida en: *Chapter 19B: Acquisition of Surveillance Technology*, del Codigo Administrativo de la ciudad de San Francisco.

[25] La sección 19B.7 de la Ordenanza citada permite a un Departamento (organismo/entidad municipal) adquirir y utilizar temporalmente "tecnología de vigilancia" exclusivamente para responder a una emergencia. Asimismo, debe dejar de usarla en un plazo de siete días o cuando termine la emergencia, conservar solo los datos relevantes y no divulgar información a terceros, a menos que sea autorizado por un tribunal o requerido por la ley. Además, deben presentar un informe a la Junta de Supervisores (concejo municipal) dentro de los 60 días posteriores al inicio de la emergencia.

[26] La Ley de Privacidad de la Información Biométrica (*Biometric Information Privacy Act,* BIPA), de 2008, de Illinois, fue una de las primeras regulaciones estatales sobre el uso comercial de FRT. En el mismo sentido, otros estados cuentan con leyes de privacidad integrales que cubren los datos de reconocimiento facial, como la Ley de Privacidad del Consumidor de California (*California Consumer Privacy Act*) (Fidler y Hurwitz, 2024).

Referencias normativas

Australia y Nueva Zelanda

Ley de Inmigración de Nueva Zelanda (*Immigration Act 2009*). Disponible en: https://www.legislation.govt.nz/act/public/2009/0051/latest/DLM1440628.html (mayo,2024).

Chile

- Ley N°19.628 sobre protección de la vida privada. Disponible en https://bcn.cl/2f7cg (mayo,2024).
- Proyecto de ley que regula la protección y el tratamiento de datos personales y crea la Agencia de Protección de Datos Personales (Boletín 11092-07 y 11144-07, refundidos). Disponible en: http://bcn.cl/3iatc (mayo,2024).
- Resolución 25425 Exenta. Dispone proceso de empadronamiento biométrico de personas extranjeras que hayan ingresado al país por paso no habilitado o eludiendo el control migratorio y se encuentren en el territorio nacional de manera irregular. Disponible en: https://www.bcn.cl/leychile/navegar/imprimir?idNorma=1193381&idVersion=2023-09-29 (mayo,2024).

Estados Unidos de América

- Ley de Seguridad Fronteriza (*Enhanced Border Security and Visa Entry Reform Act of 2002*). Disponible en: https://www.congress.gov/bill/107th-congress/house-bill/3525/text (mayo,2024).
- Proyectos de ley (nivel federal):
- *S.681 - Facial Recognition and Biometric Technology Moratorium Act of 2023 - 118th Congress (2023-2024).* Disponible en: https://www.congress.gov/bill/118th-congress/senate-bill/681 (mayo,2024).
- *H.R.1404 - Facial Recognition and Biometric Technology Moratorium Act of 2023 - 118th Congress (2023-2024).* Disponible en: https://www.congress.gov/bill/118th-congress/house-bill/1404 (mayo,2024).
- *H.R.6092 - Facial Recognition Act of 2023.* Disponible en: https://www.congress.gov/bill/118th-congress/house-bill/6092 (mayo,2024).
- Legislación municipal:
- *Chapter 19B: Acquisition of Surveillance Technology* (San Francisco). Disponible en: https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320 (mayo,2024).

Unión Europea

- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016L0680 (abril 2024).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679 (abril 2024).

Referencias generales

Australian Border Force (2019). *SmartGates*. Disponible en: https://www.abf.gov.au/entering-and-leaving-australia/smartgates (mayo,2024).

Chen, W. y Wang, M. (2023). *Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China*. *Telecommunications Policy*, *47*(2), 102482. Disponible en: https://doi.org/10.1016/j.telpol.2022.102482 (mayo,2024).

Consejo para la Transparencia, CPLT (2021). *La protección de datos personales en contextos de avanzado desarrollo tecnológico con énfasis en videovigilancia y tecnología de reconocimiento facial empleada por el sector público*: noviembre 2021. Disponible en: https://www.consejotransparencia.cl/estudios/wp-content-uploads-2022-01-la-proteccion-de-datos-personales-en-contextos-de-avanzado-desarrollo-tecnologico-con-enfasis-en-videovigilancia-y-tecnologia-de-reconocimiento-faci/ (mayo,2024).

Domingo Jaramillo, C. (2021). *Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana*. *El Criminalista Digital*, 9, 20-37. Disponible en: https://revistaseug.ugr.es/index.php/cridi/article/view/20899 (mayo,2024).

eu-LISA (s/f-a). *Who we are*. Disponible en: https://www.eulisa.europa.eu/About-Us/Who-We-Are (mayo,2024).

— (s/f-b). *Eurodac.* Disponible en: https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Eurodac (mayo,2024).

European Data Protection Board, EDPB (s/f). *Presidencia del CEPD.* Disponible en: https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_es (mayo,2024).

— (2023-a). *EDPB adopts final version of Guidelines on facial recognition technology in the area of law enforcement*. Disponible en: https://www.edpb.europa.eu/news/news/2023/edpb-adopts-final-version-guidelines-facial-recognition-technology-area-law_es (mayo,2024).

— (2023-b). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement.* Version 2.0, Adopted on 26 April 2023. Disponible en: https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (mayo,2024).

European Union Agency for Fundamental Rights, FRA (2019). *Facial Recognition technology: fundamental rights considerations in the context of law enforcement.* Disponible en: http://bcn.cl/3idfj (mayo,2024).

Fidler, M. y Hurwitz, J. (2014). *An Overview of Facial Recognition Technology Regulation in the United States.* En Matulionyte, R. y Zalnieriute, M. (Eds.), *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge University Press. Disponible en: https://doi.org/10.1017/9781009321211.011 (mayo,2024).

Hendry, J. (2022). *Home Affairs revives facial recognition plan for airports.* InnovationAus.com. Disponible en: https://www.innovationaus.com/home-affairs-revives-facial-recognition-plan-for-airports/ (mayo,2024).

Home Office (2024). *Immigration Bail,* version 19.0. Disponible en: https://assets.publishing.service.gov.uk/media/65f4260efa1851001a0117bf/Immigration+bail.pdf (mayo,2024).

Immigration New Zealand (s/f). *Biometric information*. Disponible en: https://www.immigration.govt.nz/about-us/policy-and-law/identity-information-management/how-biometric-information-is-used (mayo,2024).

Interpol (s/f). *Reconocimiento facial*. Disponible en: https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial (mayo,2024).

Iyengar, R., & Gutman-Argemí, C. (2023). *Airport immigration lines now come with facial recognition cameras*. *Foreign Policy*. Disponible en: https://foreignpolicy.com/2023/04/27/us-immigration-lines-cbp-facial-recognition/ (mayo,2024).

Kelly, N. (2022). *Facial recognition smartwatches to be used to monitor foreign offenders in UK*. *The Guardian*. Disponible en: https://www.theguardian.com/politics/2022/aug/05/facial-recognition-smartwatches-to-be-used-to-monitor-foreign-offenders-in-uk (mayo,2024).

Khan, N. y 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.jjimei.2021.100049 (mayo,2024).

Kostka, G., Steinacker, L. y Meckel, M. (2023). *Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. Government Information Quarterly*, *40*(1), 101761. Disponible en: https://doi.org/10.1016/j.giq.2022.101761 (mayo,2024).

Kuhlmann, S. (2024). *Facial Recognition Technology across the Globe: Jurisdictional Perspectives.* En Matulionyte, R. y Zalnieriute, M. (Eds.), *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge University Press. Disponible en: https://doi.org/10.1017/9781009321211.011 (mayo,2024).

Laperruque, J. (2022). *Limiting Face Recognition Surveillance: Progress and Paths Forward*. Center for Democracy and Technology. Disponible en:

https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/#:~:text=Currently%20no%20states%20have%20a,face%20recognition%20to%20track%20individuals. (mayo,2024).

Lynch, N. y Campbell, L. (2024). *Principled Regulation of Facial Recognition Technology, A View from Australia and New Zealand*. En Matulionyte, R. y Zalnieriute, M. (Eds.), The Cambridge Handbook of Facial Recognition in the Modern State. Cambridge University Press. Disponible en: https://doi.org/10.1017/9781009321211.011 (mayo,2024).

Ministry of Business, Innovation and Employment NZ (2016). *Privacy impact assessment report: Collection and handling of biometrics at the Ministry of Business, Innovation and Employment*. Disponible en: https://www.immigration.govt.nz/documents/about-us/privacyimpactassessment.pdf (mayo,2024).

Nalbandian, L. (2022). *An eye for an 'I:' a critical assessment of artificial intelligence tools in migration and asylum management*. Comparative Migration Studies, 10(1). Disponible en: https://doi.org/10.1186/s40878-022-00305-0 (mayo,2024).

National Academies of Sciences, Engineering, and Medicine (2024). *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*. Washington, DC: The National Academies Press. Disponible en: https://doi.org/10.17226/27397 (mayo,2024).

New Zealand Customs Service (2024). *eGate*. Disponible en: https://www.customs.govt.nz/personal/travel-to-and-from-nz/travelling-to-new-zealand/egate/ (mayo,2024).

Ozkul, D. (2023). *Automating Immigration and Asylum: The uses of new technologies in migration and asylum governance in Europe*. Oxford: Refugee Studies Centre, University of Oxford. Disponible en: https://www.delorscentre.eu/fileadmin/2_Research/1_About_our_research/2_Research_centres/Centre_for_Fundamental_Rights/AFAR/Automating-immigration-and-asylum_Ozkul.pdf (mayo,2024).

Pérez, S.N. (2022). *Los sistemas de reconocimiento facial: una mirada a la luz del examen de proporcionalidad*. Revista Internacional de Derechos Humanos, 12 (1). Disponible en: https://ojs.austral.edu.ar/index.php/ridh/article/view/664/987 (mayo,2024).

Privacy Commissioner (s/f). *Biometrics*. Disponible en: https://privacy.org.nz/news/consultations/biometrics (mayo,2024).

— (2021). *Can we collect biometric information?* Disponible en: https://www.privacy.org.nz/tools/knowledge-base/view/277?t=1286158_1444833 (mayo,2024).

San Francisco Police Department (2024). *19B Surveillance Technology Policies.* Disponible en: https://www.sanfranciscopolice.org/your-sfpd/policies/19b-surveillance-technology-policies (mayo,2024).

Santisteban, M. (2021). *Reconocimiento facial y protección de datos: una respuesta provisional a un problema pendiente*. Revista de Derecho UNED, 28, 499-526. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8285344 (mayo,2024).

Sarabdeen, J. (2022). *Protection of the rights of the individual when using facial recognition technology.* Heliyon, 8(3), e09086. Disponible en: https://doi.org/10.1016/j.heliyon.2022.e09086 (mayo,2024).

Servicio Nacional de Migraciones (2023). *Empadronamiento biométrico se extiende hasta fin de 2023.* Disponible en: https://serviciomigraciones.cl/empadronamiento-biometrico-hasta-fin-de-ano/#:~:text=Comparte%3A-,El%20registro%20incluye%20fotografía%20frontal%20del%20rostro%20y%20toma%20de,políticas%20públicas%20y%20en%20seguridad. (mayo,2024).

Travel.State.Gov (2024). *Safety & Security of U.S. borders: Biometrics*. Disponible en: https://travel.state.gov/content/travel/en/us-visas/visa-information-resources/border-biometrics.html#:~:text=Legal%20Requirements&text=This%20law%20requires%20that%20U.S.,documents%20that%20use%20biometric%20identifiers (mayo,2024).

U.S. Customs and Border Protection, CBP (2024). *Biometrics.* Disponible en: https://www.cbp.gov/travel/biometrics (mayo,2024).

U.S. Government Accountability Office, U.S. GAO (2024). *Facial Recognition Technology: Federal Law Enforcement Agency efforts related to civil rights and training*. Disponible en: https://www.gao.gov/products/gao-24-107372 (mayo,2024).

Utegen, D. y Rakhmetov, B. (2023). *Facial recognition technology and ensuring security of biometric data: Comparative analysis of legal regulation models.* Journal of Digital Technologies and Law, 1(3), 825-844. Disponible en: https://doi.org/10.21202/jdtl.2023.36 (mayo,2024).

Wenger, E.; Shan, S.; Zheng, H. y Zhao, B.Y. (2023). *SoK: Anti-Facial Recognition Technology*, 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, California, USA, 2023, 864-881. Disponible en: https://ieeexplore.ieee.org/abstract/document/10179445 (mayo,2024).

Wienroth, M. y Amelung, N. (2023). '*Crisis', control and circulation: Biometric surveillance in the policing of the 'crimmigrant other*.' International Journal of Police Science & Management, 25(3), 297-312. Disponible en: https://journals.sagepub.com/doi/full/10.1177/14613557231184696 (mayo,2024).

Nota aclaratoria

Asesoría Técnica Parlamentaria está enfocada en apoyar preferentemente el trabajo de las Comisiones Legislativas de ambas Cámaras, con especial atención al seguimiento de los proyectos de ley. Con lo cual se pretende contribuir a la certeza legislativa y a disminuir la brecha de disponibilidad de información y análisis entre Legislativo y Ejecutivo.