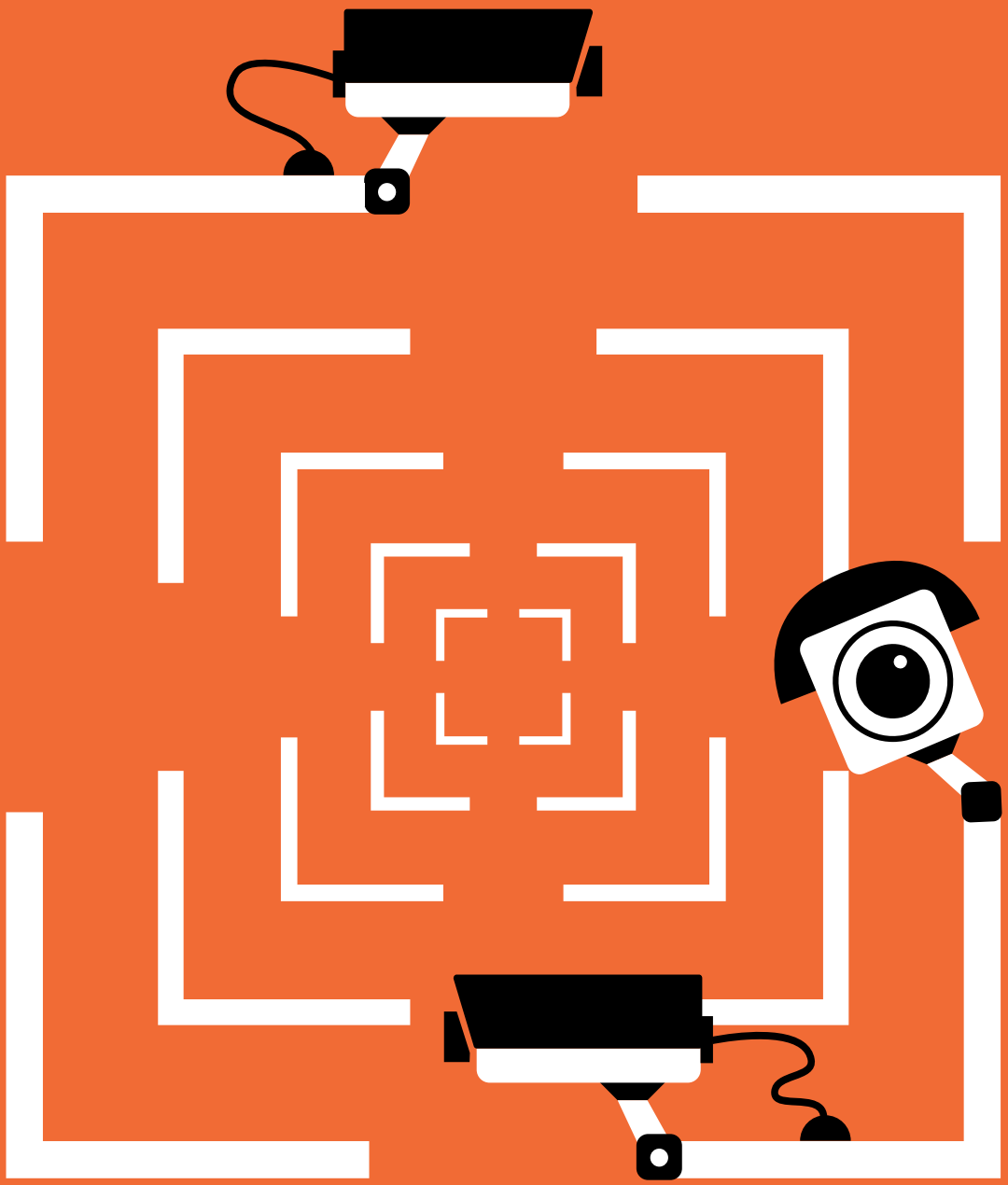
Fuera de control

USO POLICIAL DEL RECONOCIMIENTO FACIAL AUTOMATIZADO EN URUGUAY



Datysoc
LABORATORIO DE
DATOS Y SOCIEDAD

Texto: Patricia Díaz Charquero

Portada y diagramación: Estudio Carolina Curbelo + Amparo Bengochea

Revisión: Javier Preciozzi y Matías Jackson

Edición: Jorge Gemetto

Marzo de 2022

Esta publicación cuenta con el apoyo de:

DERECHOS DIGITALES América Latina

INDELA

Índice

Glosario de siglas y acrónimos

Agesic - Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento

CCTV - Circuito Cerrado de Televisión

CCU - Centro de Comando Unificado del Ministerio del Interior

DIMOE - Dirección de Monitoreo Electrónico del Ministerio del Interior

DNIC - Dirección Nacional de Identificación Civil

IA - Inteligencia artificial

MI - Ministerio del Interior

NIST - National Institute of Standards and Technology

RFA - Reconocimiento facial automatizado

SGSP - Sistema de Gestión de Seguridad Pública del Ministerio del Interior

SIVVE - Sistema Integrado de Videovigilancia y Emergencia del Ministerio del Interior

URCDP - Unidad Reguladora y de Control de Datos Personales

US GAO - United States Government Accountability Office

Introducción

En los últimos años, las tecnologías de reconocimiento facial automatizado (RFA) han experimentado un enorme crecimiento. Sus usos en diferentes contextos se han disparado, especialmente aquellos relacionados con seguridad y vigilancia. Los beneficios potenciales de su uso por parte de las fuerzas policiales, como la prevención o disuasión en actividades delictivas y la capacidad de encontrar a personas de interés, se ven atenuados por los riesgos de vigilancia masiva, el impacto desigual en grupos vulnerables y la falta de consentimiento de la ciudadanía.

Frente a la reciente adquisición de un software de RFA por la fuerza policial uruguaya y la creación de una base biométrica con datos de identificación facial de todos los ciudadanos y ciudadanas mayores de edad para su uso con fines de seguridad pública, se hace necesario contar con la mayor cantidad de información posible para lograr un debate social informado en torno a su uso. Con este informe pretendemos aportar elementos para el debate, explicando aspectos básicos sobre el funcionamiento del RFA y el estado actual de su regulación en Uruguay.

El informe se estructura en tres partes, un apartado de conclusiones y un anexo. La primera parte presenta las definiciones y conceptos básicos para comprender el funcionamiento del RFA. En la segunda parte se analizan los escenarios de uso del RFA en el marco de procedimientos policiales y los principales desafíos que presenta su uso desde el marco de los derechos humanos. En la tercera parte se reporta sobre el uso de sistemas de RFA por la policía en Uruguay. Por último, se presentan las conclusiones, incluyendo recomendaciones de políticas públicas y propuestas específicas de acción. El anexo reúne documentación que respalda la investigación.

Las dos primeras partes del informe son el resultado de un relevamiento del estado del arte y de la normativa sobre el tema, mientras que para analizar el uso de sistemas de RFA por la policía en Uruguay se condujeron entrevistas con informantes calificados y con personal de la Unidad Reguladora y de Control de Datos Personales (URCDP) de Uruguay. Estas entrevistas se complementan con solicitudes de acceso a la información pública presentadas ante el Ministerio del Interior (MI) y la URCDP.

1. ¿Qué es el RFA y cómo funciona?

La tecnología de reconocimiento facial automatizado utiliza una o más fotos o imágenes fijas de una transmisión de video de una persona y las convierte en una plantilla facial o una representación matemática de la imagen. Luego, un algoritmo (es decir, un conjunto de instrucciones) que calcula el grado de coincidencia puede comparar esa plantilla con una plantilla generada a partir de otra foto. De esta manera, puede determinar el nivel de similitud. Las plantillas pueden almacenarse de forma independiente de las imágenes de los rostros.

Gráfico 01.

Los sistemas más modernos de RFA se basan en el aprendizaje automático, una rama de la inteligencia artificial (IA). El algoritmo utiliza datos de entrenamiento (fotos de rostros) para identificar patrones y determinar de forma automatizada las partes de cada rostro que son importantes para averiguar quién es cada persona en particular. En los últimos años se utilizan redes neuronales profundas, un tipo especial de algoritmo de aprendizaje automático, para volver más precisos los sistemas y lograr que "aprendan" a reconocer nuevos rostros.[1]

1.1. Tipos y usos de sistemas de biometría facial

No todos los usos de la biometría facial implican RFA propiamente dicho. El RFA suele referirse a dos tipos de operaciones: la verificación facial y la identificación facial.

1 Patrick Grother, Mei Ngan, y Kayee Hanaoka, «Ongoing Face Recognition Vendor Test (FRVT) Part 2:: Identification» (Gaithersburg, MD: National Institute of Standards and Technology, noviembre de 2018), p.2, https://doi.org/10.6028/NIST.IR.8238

En la siguiente tabla se sintetizan los principales tipos y usos de sistemas de biometría facial. Se resaltan en color aquellos que corresponden al RFA.

DETECCIÓN FACIAL	VERIFICACIÓN FACIAL	IDENTIFICACIÓN FACIAL	ANÁLISIS FACIAL
Responde a la pregunta: ¿esto es un rostro?	Responde a la pregunta: ¿es esta persona quien dice ser?	Responde a la pregunta: ¿quién es esta persona?	Responde a varias preguntas posibles: ¿qué edad tiene esta persona?, ¿de qué sexo es?, ¿qué está sintiendo?, entre otras.
Este sistema detecta que existe un rostro. Lo hace buscando la forma general de un rostro humano sin identificarlo.	Es un sistema de coincidencia uno a uno en el que se compara la imagen del rostro que se desea verificar con la plantilla facial o la imagen guardada de una persona.	Es un sistema de coincidencia uno a muchos (1 a N) que compara una imagen de un rostro con una galería de plantillas faciales o imágenes de un banco de personas que tienen sus datos de identificación.	Es una tecnología distinta del reconocimiento facial. El análisis facial utiliza la imagen de un rostro para estimar o clasificar características personales como la edad, la raza o el género.
Suele usarse como paso previo a la verificación o identificación facial, o para realizar seguimiento sin identificar a las personas. Un ejemplo es cuando en un shopping se realiza el seguimiento del tráfico peatonal para analizar los flujos de clientes y así conocer cuáles son las horas pico, a dónde van los clientes y cuánto tiempo permanecen.	Suele usarse con fines de acceso seguro. Por ejemplo, para desbloquear aplicaciones o dispositivos o para ingresar a locales de trabajo, como medio de pago o inclusive para controlar la asistencia en universidades.	Suele usarse con fines de seguridad para vigilar espacios públicos, ya sea por la policía o por actores privados (por ejemplo, se usa en casinos para detectar tramposos conocidos y miembros de redes del crimen organizado, así como en estadios deportivos para detectar el ingreso de personas con antecedentes de violencia). También se usa en algunos servicios web y redes sociales para etiquetar y organizar fotografías.	Suele usarse para analizar características o acciones de las personas. Por ejemplo, para acelerar la identificación de la edad de un cliente con el fin de comprar sustancias controladas, como el alcohol, o para analizar las reacciones de los candidatos en procesos de contratación laboral.

En este informe nos centraremos en las funciones de detección, verificación e identificación facial (ver Gráfico 2), dado que son las más comunes.

Gráfico 02.

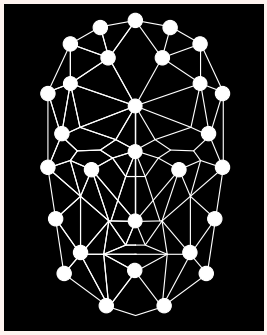
PASO 01. CAPTURA

Una cámara captura una imagen o un video, que luego se utiliza para alimentar el sistema. Puede tratarse de una captura en vivo o de una grabación previa.

PASO 02. DETECCIÓN DE ROSTROS

El sistema busca la presencia de los rasgos generales de un rostro humano y los encuentra.

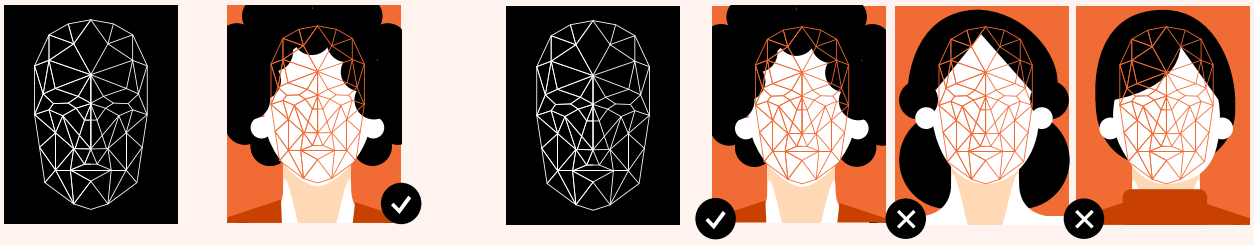
PASO 03. CREACIÓN DE PLANTILLA FACIAL



El sistema ajusta diferentes parámetros (iluminación, poses, etc.) y crea una plantilla especial para ese rostro extrayendo sus rasgos distintivos.

PASO 04. BÚSQUEDA DE COINCIDENCIAS:

Una vez generada la nueva plantilla facial, el sistema la usa con propósitos de verificación o de identificación:



Verificación: coincidencia uno-a-uno. La imagen en vivo es comparada con una imagen almacenada para verificar una identidad. Esto ocurre, por ejemplo, en los controles migratorios de aeropuertos.

Identificación: coincidencia uno-a-muchos. Se compara una imagen capturada con una galería de imágenes para encontrar una o varias potenciales coincidencias. Se usa, por ejemplo, cuando el fin es identificar a un individuo desconocido en la escena de un crimen.

1.2. Requisitos para aplicar RFA

El uso de RFA requiere:

- *Una forma de capturar imágenes.* Por ejemplo, mediante un circuito cerrado de televisión (CCTV) o cualquier dispositivo que permita capturar una imagen o video (celulares, cámaras fotográficas, etc.). También pueden utilizarse imágenes previamente capturadas y almacenadas (en sitios web, redes sociales, etc.).

- *Un software* que utilice un algoritmo para procesar la imágenes, detectar rostros, generar la plantilla biométrica correspondiente y almacenarla en una base biométrica, para luego compararla con otras plantillas (verificación o identificación).
- *Una base de datos de referencia*, es decir, una galería de fotos de rostros (usualmente con identidades confirmadas) controlada por quien opera el sistema. Estas fotos de referencia son almacenadas en el sistema con fines de comparación.
- *Una base legal para su uso*. En la mayoría de los países del mundo, los datos biométricos se consideran datos personales sensibles, por lo que, para que estos puedan ser utilizados, requieren el previo consentimiento informado de la persona o una ley que lo habilite cumpliendo con requisitos especiales.

1.3. Definiciones

Para una primera aproximación al funcionamiento del RFA, brindaremos algunas definiciones de interés (actores, precisión, ambiente, desempeño, sesgos y umbrales) contenidas principalmente en los informes del National Institute of Standards and Technology (NIST)[2] [3] y de la United States Government Accountability Office (US GAO).[4] [5] [6] También incluímos algunos antecedentes e investigaciones recientes sobre el tema.

1.3.1. Actores

Las partes involucradas en el uso de sistemas de RFA suelen ser las siguientes:

2 El NIST es el Instituto de Estándares y Tecnología del Departamento de Comercio de los Estados Unidos. Presenta informes periódicos en el marco del programa de Prueba de Proveedores de Reconocimiento Facial (FRVT).

3 NIST, Projects, «Face Recognition Vendor Test (FRVT)», NIST, 8 de julio de 2010 (actualizada el 30 de noviembre de 2020). https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

4 La U.S. GAO elabora informes para el Congreso y para los jefes de las agencias de gobierno de Estados Unidos.

5 U.S. Government Accountability Office, «Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses», Report to Congressional Requesters, julio de 2020. https://www.gao.gov/assets/gao-20-522.pdf

6 U.S. Government Accountability Office, «Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks», 3 de junio de 2021. https://www.gao.gov/products/gao-21-518

- Desarrolladores: empresas que crean algoritmos de reconocimiento facial.
- Proveedores o *vendors*: empresas que aprovechan los algoritmos de reconocimiento facial que ellos u otros han desarrollado para ofrecer productos o servicios orientados al consumidor o usuario final. También suelen ofrecer servicios de CCTV.
- Usuarios finales: suelen ser empresas (públicas o privadas) u organismos gubernamentales que utilizan tecnología de reconocimiento facial y también los consumidores y consumidoras en general cuando utilizan RFA en sus dispositivos personales.

1.3.2. Precisión o desempeño

El desempeño de un sistema se refiere al grado de satisfacción o utilidad que se obtiene con respecto a la información que recibe. El desempeño se suele medir e informar con los siguientes conceptos:

- *Falso positivo*: declarar incorrectamente que dos imágenes son una coincidencia cuando en realidad son de dos personas diferentes.
- *Falso negativo*: no declarar que dos imágenes coinciden cuando en realidad son de la misma persona.
- *Tasa de fallo en la inscripción*: la proporción de imágenes faciales en las que el algoritmo no puede detectar un rostro o crear una plantilla facial y, por lo tanto, no puede realizar la verificación (1 a 1) o la identificación (1 a N).

La literatura técnica utiliza los términos *desempeño diferencial* o *diferenciales demográficos* cuando un algoritmo tiene diferencias de desempeño o precisión al procesar información de distintos grupos demográficos. Por ejemplo, si la tasa de falsos negativos es mayor en mujeres que en hombres. Estos diferenciales pueden constituir un tipo de *sesgo algorítmico* (ver 1.3.6. Sesgos).

1.3.3. Ambiente controlado vs. ambiente no controlado

Los sistemas de RFA se pueden utilizar en diferentes contextos o escenarios, como en aeropuertos, bares o en las calles. Un *ambiente controlado* es aquel en el que se pueden controlar factores importantes como la iluminación, el fondo y la posición del rostro. Por ejemplo, en el control migratorio de un aeropuerto. Un *ambiente no controlado* (en inglés se usa el término *on the wild*) es el mundo real, donde los factores pueden variar, lo que plantea desafíos particulares a los algoritmos de reconocimiento facial.

1.3.4. Pruebas de desempeño vs. desempeño en ambientes no controlados

El error más común, cuando se habla de pruebas de desempeño de un sistema de RFA, es suponer que las pruebas estándar serán representativas del desempeño del sistema en ambientes no controlados (el mundo real). Como hemos visto, existen muchos factores que pueden incidir sobre el desempeño de un sistema de RFA en el mundo real. Por ejemplo, en estudios recientes,[7] profesionales del NIST descubrieron que, cuando las pruebas se realizan sobre imágenes de rostros pertenecientes a una población diversa de personas de varios países y grupos de edad, las tasas de falsos positivos son muy bajas (alrededor de 1 en 10.000). Cuando las pruebas se realizan sobre una población más homogénea, donde la comparación se realiza entre personas del mismo grupo de edad y área geográfica, la tasa de falsos positivos aumenta unas 20 veces. Esta discrepancia se produce porque, cuando las personas tienen la misma edad o comparten más rasgos, pueden ser más difíciles de distinguir.

En definitiva, el rendimiento de un sistema depende en gran medida de las circunstancias en las que se implementa y la tasa de error obtenida en pruebas estándar es simplemente un punto de referencia y no una predicción exacta de cómo se comportará el sistema en un contexto dado, por lo que no debe usarse de forma aislada para justificar el uso del sistema.

7 Patrick Grother, Mei Ngan, y Kayee Hanaoka, «Face Recognition Vendor Test Part 3:: Demographic Effects» (Gaithersburg, MD: National Institute of Standards and Technology, diciembre de 2019). https://doi.org/10.6028/NIST.IR.8280

1.3.5. Factores que influyen en la precisión

Los *factores físicos* están relacionados con las características intrínsecas de un rostro y con el proceso mediante el que se captura la imagen de ese rostro. Pueden incluir los siguientes:

- Pose, iluminación o expresión del rostro.
- Cosméticos, anteojos, cabello, mascarillas u otros aspectos cambiantes que pueden cubrir partes de la cara.
- Calidad general de la imagen, dependiente del entorno no controlado, la distancia o la configuración de la cámara, entre otros factores.
- Características faciales inherentes, particularmente la reflectancia de la piel y la estructura facial subyacente.
- Envejecimiento u otras diferencias entre la imagen de referencia y la imagen actual de una persona.

Los *factores relacionados con el algoritmo* dependen de cómo fue creado y cómo funciona un algoritmo de reconocimiento facial. Pueden incluir los siguientes:

- Propósito del algoritmo (por ejemplo, identificación o verificación).
- Tipo de algoritmo, como redes neuronales profundas modernas frente a algoritmos antiguos no entrenables.
- Datos utilizados para entrenar el algoritmo. Esto incluye la cantidad de imágenes que se usan, los grupos demográficos representados en las imágenes y la representación de los factores físicos mencionados anteriormente (por ejemplo, datos de entrenamiento que incluyan personas con tapaboca, personas maquilladas, imágenes de diferente calidad, etc.).
- Configuración de umbrales operativos (ver 1.3.7. Puntajes de similitud y manejo de umbrales).
- La base biométrica con la que actúa el algoritmo, es decir, la base de datos de referencia que utiliza el usuario final para comparar. Un sistema biométrico siempre debe considerarse junto con la base con la que actúa: por más preciso que sea el

algoritmo, si la base biométrica es de mala calidad, aumentarán los errores. Este factor es determinante del desempeño de un sistema de RFA.

1.3.6. Sesgos

El *sesgo algorítmico* se produce cuando un algoritmo muestra un prejuicio o inclinación por un resultado sobre otro creando errores sistemáticos y repetitivos en un sistema informático. Esto conduce a resultados injustos, como privilegiar a un segmento demográfico sobre otro.

Quizá los tres estudios más conocidos en relación al sesgo de algoritmos de reconocimiento facial son el realizado por Buolamwini y Gebru en el año 2018,[8] los realizados por Patrick Grother y su equipo del NIST, especialmente el publicado en el año 2019,[9] y el resumen general de sesgos demográficos en biometría publicado en 2020 por Drozdowski *et al.*[10]

Buolamwini y Gebru evaluaron 3 algoritmos de RFA comerciales y encontraron que todos funcionaban mejor para individuos de piel más clara y para hombres en general. La tasa máxima de error para hombres de piel clara es de 0,8 %, mientras que el peor desempeño corresponde a la detección de rostros de mujeres de piel más oscura, con tasas de error de hasta 34,7 %. Concluye que las disparidades sustanciales en la precisión entre hombres-mujeres y piel blanca-oscura "requieren atención urgente si las empresas comerciales quieren construir algoritmos de análisis facial genuinamente justos, transparentes y responsables" (traducción nuestra).

Los últimos informes de evaluación del NIST dan cuenta de una mejora sostenida y significativa en la precisión de los algoritmos de reconocimiento facial desde el año 2000 a la fecha, pero encontraron que existen diferencias de desempeño para ciertos grupos

8 Joy Buolamwini y Timnit Gebru, «Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification», en *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (Conference on Fairness, Accountability and Transparency, PMLR, 2018), 77-91. https://proceedings.mlr.press/v81/buolamwini18a.html

9 Ob. cit. nota 3.

10 Pawel Drozdowski et al., «Demographic Bias in Biometrics: A Survey on an Emerging Challenge», *IEEE Transactions on Technology and Society* 1, n.º 2 (junio de 2020): 89-103. https://doi.org/10.1109/TTS.2020.2992344

demográficos. El equipo del NIST publicó a finales de 2019 un análisis exhaustivo del desempeño en diferentes grupos demográficos de 189 algoritmos de reconocimiento facial de 99 desarrolladores. El NIST descubrió que los rostros asiáticos y africanos obtenían coincidencias de falsos positivos entre 10 y 100 veces más a menudo que los rostros de las personas blancas. Al igual que Buolamwini y Gebru, encontraron que las mujeres afroamericanas experimentaron las tasas más altas de falsos positivos. "Las diferencias en los falsos positivos en la comparación de uno a muchos son particularmente importantes porque las consecuencias podrían incluir acusaciones falsas", expresa el equipo del NIST en el resumen del informe sobre los efectos demográficos del RFA.[11]

En definitiva, el sesgo existe y también se ha detectado sobre quiénes recae, aunque aún no es claro qué factores lo causan. La US GAO concluye que no hay consenso entre la academia, los desarrolladores y los organismos independientes de evaluación sobre cómo corregir los sesgos detrás de estas diferencias de desempeño que podrían tener consecuencias sobre la vida de las personas, especialmente de algunos grupos demográficos. Por su parte, el equipo del NIST aclara que su metodología no analiza causa y efecto, por lo que no intenta explicar o inferir las razones técnicas de los resultados que documenta.

Existe abundante literatura que indica que la paridad estadística y la amplitud de las etnias utilizadas en los datos de entrenamiento de los algoritmos suelen ser un factor especialmente relevante para el desempeño del reconocimiento facial. Estos estudios (incluyendo los del NIST[12] y la US GAO)[13] hablan del *efecto otra raza*. Se trata de la constatación de que las personas identifican mejor a los individuos de su propia raza o etnia debido a una mayor exposición a ellos. Algo similar ocurre con los algoritmos. Así, los estudios encuentran que los algoritmos de reconocimiento facial desarrollados en países asiáticos son mejores para reconocer caras de asiáticos y los algoritmos occidentales son en promedio mejores para reconocer rasgos caucásicos. De cualquier forma, el desempeño de un sistema de RFA depende de

11 U.S. Department of Commerce, National Institute of Standards and Technology (NIST), «NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software», NIST News, 19 de diciembre de 2019. https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

12 Ob. cit. nota 3.

13 Ob. cit. nota 5.

múltiples factores relacionados con el diseño y configuración del algoritmo, así como de factores físicos. El problema que enfrentan los equipos académicos y de evaluación es que las pruebas se realizan sobre "cajas negras", porque los desarrolladores no comparten el código ni los datos de entrenamiento, por considerarlos propietarios y confidenciales.

Finalmente, vale la pena señalar que cada vez más reglamentaciones establecen que los sistemas de RFA deben diseñarse para permitir la *supervisión por parte de humanos*, quienes tienen la tarea de prevenir o minimizar los riesgos derivados de las posibles deficiencias del algoritmo. En este punto es central comprender que, al introducir el factor humano, se deben instrumentar estrategias para prevenir otro tipo de sesgo: el *sesgo cognitivo*. Si bien la intervención humana es necesaria, no siempre es suficiente para corregir o advertir errores de desempeño en los algoritmos. Muchas veces la confianza acrítica en las herramientas automatizadas por parte de quienes operan con ellas implica otros riesgos. Entre estos riesgos se encuentran la sobrevaloración de la información que brinda el sistema y el procesamiento selectivo de la información, en el que se descarta información alternativa relevante para identificar a un individuo (*sesgo de confirmación*).[14]

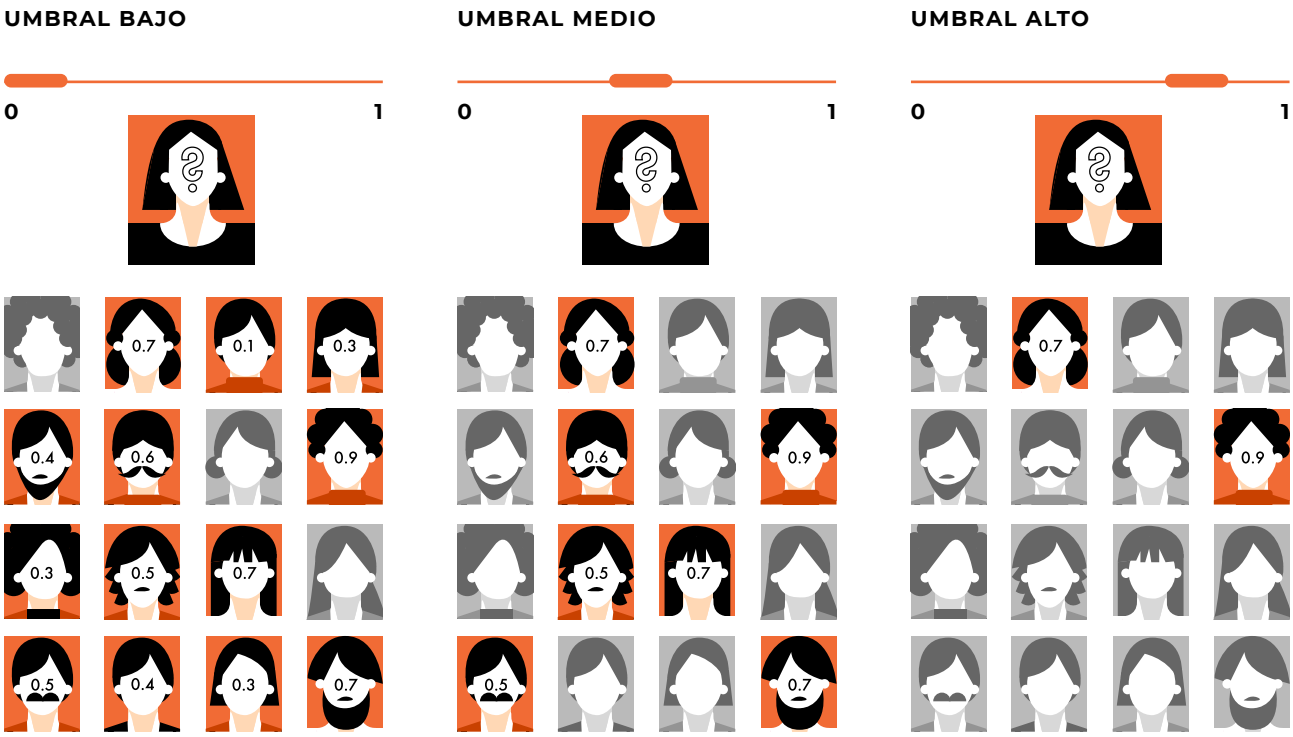
1.3.7. Puntajes de similitud y manejo de umbrales

Al momento de la verificación o identificación de una persona, los sistemas de RFA realizan una comparación entre dos caras. El resultado de esta comparación es un puntaje de qué tan probable es que esas dos imágenes sean de la misma persona: cuanto mayor sea el puntaje, más probable es que sea la misma.

Ahora bien, dado un puntaje, ¿cómo decidir si se acepta o no una comparación como válida? Dicho de otra forma: ¿a partir de qué valor de puntaje se debería dar por válida la comparación y a partir de cuál rechazarla? Esta respuesta se establece mediante la definición de un umbral: si la comparación da un puntaje mayor, se acepta, y si da un puntaje menor, se rechaza.

14 Ben Green y Amba Kak, «The False Comfort of Human Oversight as an Antidote to A.I. Harm», *Slate*, 15 de junio de 2021. https://slate.com/technology/2021/06/human-oversight-artificial-intelligence-laws.html

Gráfico 03.



Una vez definido el umbral, se presentan dos tipos de errores, vistos anteriormente:

- comparaciones correctas que son rechazadas por obtener un puntaje menor al umbral (falsos negativos)
- comparaciones incorrectas que son aceptadas por el sistema, ya que su puntaje es mayor al umbral (falsos positivos).

El umbral se puede ajustar para disminuir una u otra tasa de error, pero siempre habrá un compromiso. Estos umbrales suelen definirse sobre bases de datos conocidas, donde se pueden hacer comparaciones y sacar estadísticas de falsos positivos y falsos negativos.

En la práctica, los umbrales se configuran en función de las necesidades del usuario final, del contexto de uso y de las consecuencias asignadas a un *match* o coincidencia. Por ejemplo, si se usa RFA en un sistema de seguridad para la identificación de personas que ingresan a un edificio que almacena armas o materiales peligrosos, es probable que el usuario final esté más dispuesto a enfrentar situaciones de falsos negativos. Si el RFA se usa con fines de marketing para ofrecer productos a clientes VIP que han consentido recibir notificaciones de ofertas mientras recorren un shopping, es posible que el usuario final esté más dispuesto a enfrentar situaciones de falsos positivos. También es usual la práctica de definir un umbral mínimo y otro máximo: si el puntaje es menor al mínimo

se rechaza, si es mayor al máximo se acepta, pero si cae en el medio se dispara un proceso alternativo (por ejemplo, un chequeo manual).

Resulta evidente la importancia de que los usuarios finales sepan que tienen la opción de ajustar el umbral y que reciban la formación adecuada por parte de los proveedores o desarrolladores para hacerlo correctamente de acuerdo al contexto y a los diferentes escenarios de uso.

1.4. Principales controversias frente al uso de RFA

Los problemas generales que se detectan hoy en relación al uso de RFA, según la US GAO,[15] son:

- *Los problemas de privacidad y seguridad sobre los datos*. Se da la imposibilidad de control efectivo de las personas sobre sus datos biométricos y sobre la información personal asociada a ellos. Esta imposibilidad es inherente al propio desarrollo de los algoritmos, que implica el uso de grandes volúmenes de imágenes de personas como datos de entrenamiento.[16] Los datos de biometría facial son datos sensibles dado que las personas no pueden ocultarlos.
- *Los problemas en la precisión y el desempeño* (tasas de falsos negativos y falsos positivos). Como hemos visto, existen muchos estudios que alertan sobre los sesgos en el funcionamiento de los sistemas de RFA que podrían perjudicar a diferentes segmentos de la población, especialmente a personas con tez oscura, mujeres, niños y niñas, personas adultas mayores y personas trans.
- *Los problemas de opacidad*. Los organismos evaluadores de los algoritmos no tienen acceso al código ni a los datos utilizados para entrenar los algoritmos, porque estos son propiedad de las empresas y no se comparten con evaluadores ni con el público. Como vimos, debido a este efecto "caja negra", no existe consenso sobre cuáles son los factores que podrían causar diferencias de desempeño para ciertos datos demográficos.

15 United States Government Accountability Office, 2020. «Facial Recognition Technology. Privacy and Accuracy Issues Related to Commercial Uses». Report to Congressional Requesters. https://www.gao.gov/assets/gao-20-522.pdf

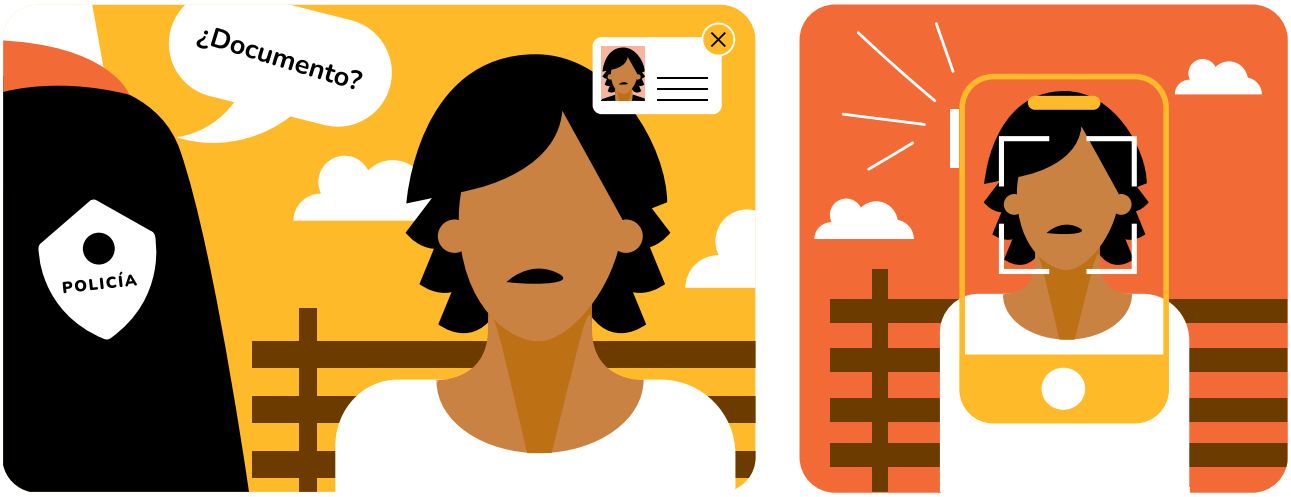
16 Ver, por ejemplo, el proyecto Exposing.ai, que muestra qué fotos de Flickr fueron utilizadas en proyectos de vigilancia biométrica. Adam Harvey y Jules Laplace, «Flickr photo face recognition dataset search», Exposing.ai, accedido el 18 de febrero de 2022. https://exposing.ai/search/

2. Uso policial de RFA desde la perspectiva de los derechos humanos

2.1. Escenarios de uso policial de sistemas de RFA

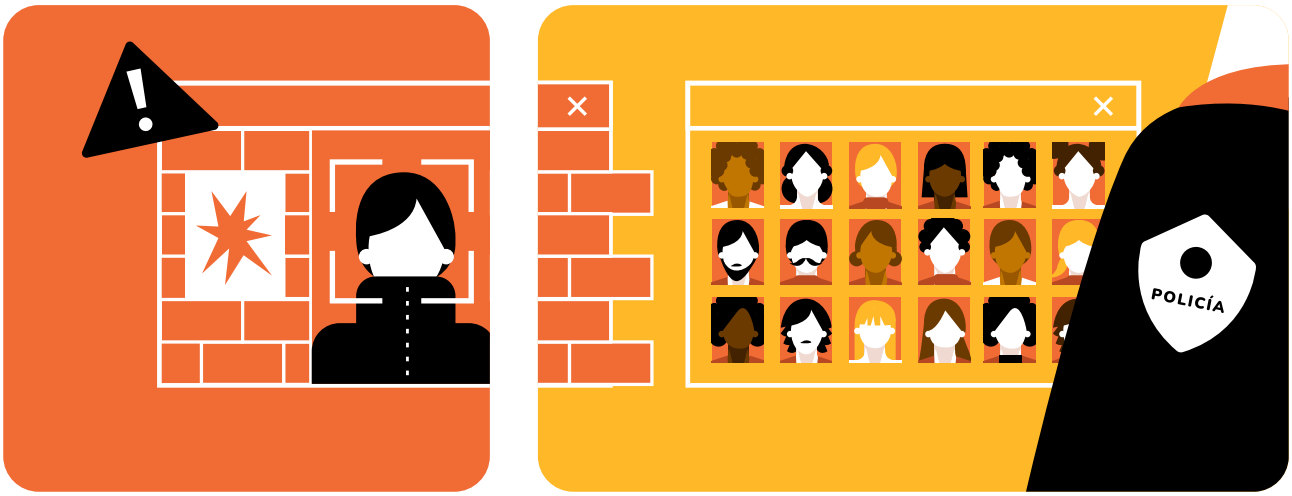
El RFA puede ser utilizado por la policía al menos de cuatro formas generales:

a) Confirmar la identidad de un individuo.



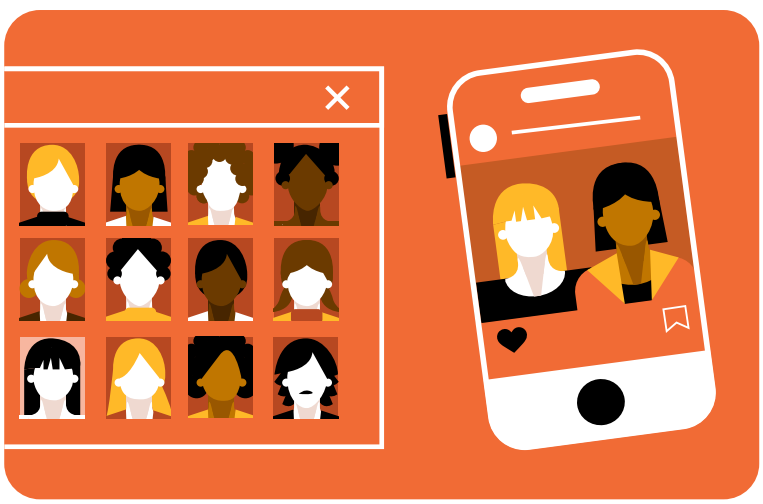
La policía requiere que una persona se identifique y esta se niega a dar su nombre o carece de documentación que acredite su identidad declarada. La policía, entonces, toma una "imagen de prueba" estática del rostro del individuo. Luego, el software de RFA se usa para verificar la identidad declarada (1 a 1) o identificar al individuo comparando esa imagen con una base de datos de imágenes que la policía controla o a la que tiene acceso (1 a N).

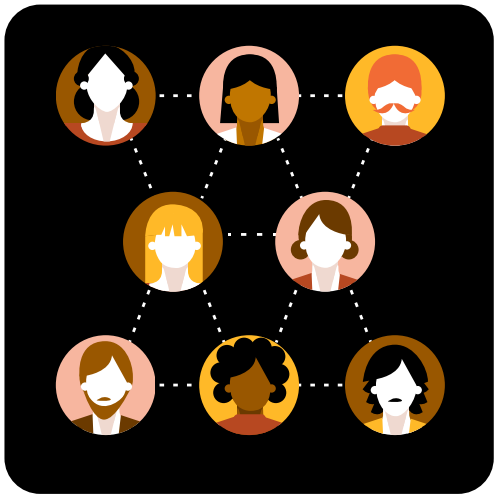
b) Identificación retrospectiva o forense.



Las imágenes de videovigilancia muestran a un presunto ladrón saliendo de una propiedad. Una imagen fija del rostro del sospechoso se utiliza como imagen de prueba y se compara con una base de datos de imágenes de custodia. El software de RFA genera una lista corta de posibles coincidencias y la policía arresta a un sospechoso basándose en que su lugar de residencia está cerca de la escena del robo y en que el grado de coincidencia del RFA es alto.

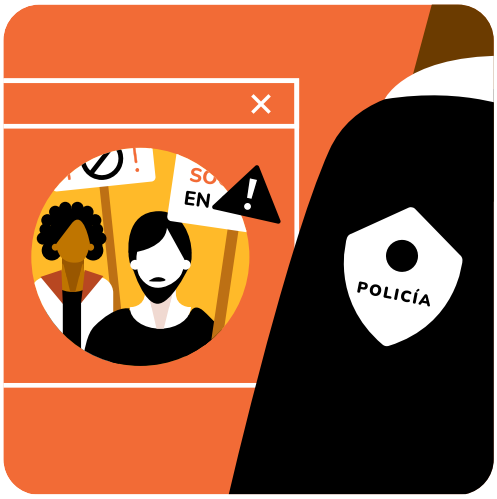
c) Cibervigilancia.





El RFA se usa como método de prevención del delito a través de la vigilancia de fuentes abiertas en internet. En este caso la policía toma imágenes publicadas en internet (por ejemplo, en redes sociales) y usa el software de RFA para averiguar la identidad y los vínculos de las personas que aparecen en las fotografías, en el marco de actividades de inteligencia criminal.

d) RFA en vivo.



Se utiliza un despliegue en vivo de RFA para identificar a "personas de interés" en el espacio público. Por ejemplo, puede usarse para tratar de identificar prófugos de la justicia o personas desaparecidas. El RFA en vivo generalmente implica la instalación de cámaras de vigilancia para capturar imágenes de personas en espacios públicos, que luego se comparan con imágenes de personas en una o varias "listas de vigilancia" compiladas por la policía.

2.2. Vigilancia y derechos humanos

Los sistemas nacionales de identificación no son nuevos y se han utilizado para diversos fines. Bases de huellas dactilares, de rostros, de matrículas de automóviles o padrones de telefonía móvil vienen siendo utilizados como insumo para diferentes herramientas informáticas gubernamentales que, a su vez, interoperan fácilmente. Lo que ha elevado las alarmas a nivel mundial es la capacidad cada vez mayor de intrusión del Estado en materia de vigilancia mediante el aumento de la capacidad de recolección y almacenamiento de datos, la inclusión de nuevas capas de seguimiento y el alto nivel de interoperabilidad que poseen las nuevas tecnologías.

Cuando las tecnologías de vigilancia se utilizan con fines de seguridad pública, deben respetar de forma estricta el marco internacional de derechos humanos. Las prácticas de control y vigilancia por parte de los gobiernos afectan directamente derechos como la libertad de expresión, la privacidad, el derecho de reunión o el derecho a la protesta o manifestación pacífica, tanto en espacios físicos como en línea.[17]

Como estos derechos no son absolutos, el Comité de Derechos Humanos de la ONU[18] interpreta de forma unánime que se permitirá la adopción de medidas de vigilancia sobre la ciudadanía siempre que:

a. estén autorizadas por una ley nacional que sea accesible, precisa y que proporcione salvaguardas eficaces contra un uso excesivo, ajustándose a los requisitos del Pacto Internacional de Derechos Civiles y Políticos,

17 Comité de Derechos Humanos de las Naciones Unidas, «Observación General No. 37», Pub. L. No. CCPR/C/GC/37, accedido 1 de febrero de 2022. https://undocs.org/es/CCPR/C/GC/37

18 Ben Emmerson, «Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo», A/69/397, párr. 30. (Naciones Unidas, 2014). https://undocs.org/es/A/69/397

b. tengan un objetivo legítimo, y

c. cumplan los criterios de necesidad y proporcionalidad.

> **Necesidad:** "un medio es necesario cuando no pudo ser establecido otro medio, igualmente adecuado para el logro del fin, pero que suponga una menor restricción para el derecho fundamental afectado."
>
> **Proporcionalidad:** la limitación al derecho fundamental debe "guardar una relación razonable con el peso e importancia de los argumentos que hablan a favor de una mayor y mejor protección del derecho afectado."
>
> Clérico, 2020 (p.28)[19]

Un requisito previo para la aplicación del test de necesidad y proporcionalidad es contar con la información necesaria para analizar cómo se implementa el uso policial de estas tecnologías. Ya en el año 2014 la Alta Comisionada de las Naciones Unidas para los Derechos Humanos advierte que los Estados suelen usar sistemas de vigilancia de forma opaca, sin leyes nacionales adecuadas, sin garantías procesales y sin suficiente supervisión. La Alta Comisionada denuncia "la preocupante falta de transparencia gubernamental asociada a las políticas, leyes y prácticas de vigilancia, que dificulta todo intento de evaluar su compatibilidad con el derecho internacional de los derechos humanos y asegurar la rendición de cuentas".[20] Y en su informe de julio de 2020,[21] directamente desaconseja el uso de sistemas de RFA, especialmente en espacios públicos o cuando exista un marco de regulación y supervisión débil o incluso ninguno.

Por su parte, el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión realiza en 2019 un llamado urgente para la rigurosa regulación

19 Laura Clérico, *Derechos y proporcionalidad: violaciones por acción, por insuficiencia y por regresión. Miradas locales, interamericanas y comparadas.* (Instituto de Estudios Constitucionales del Estado de Querétaro, 2020).

20 Alto Comisionado de las Naciones Unidas para los Derechos Humanos, «Informe sobre el derecho a la privacidad en la era digital», A/HRC/27/37, párr. 48. (Asamblea General de las Naciones Unidas, 30 de junio de 2014), https://undocs.org/es/A/HRC/27/37

21 Alto Comisionado de las Naciones Unidas para los Derechos Humanos, «Informe sobre el impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas», A/HRC/44/24, parr. 38. (Asamblea General de las Naciones Unidas, 24 de junio de 2020), https://undocs.org/es/A/HRC/44/24

de las exportaciones de equipos de vigilancia, la adopción de restricciones más estrictas para su utilización, y solicita una moratoria inmediata sobre la venta y la transferencia a nivel mundial "hasta que se establezcan estrictas salvaguardas de los derechos humanos en la regulación de esas prácticas y se pueda garantizar que los gobiernos y los agentes no estatales van a utilizar esos instrumentos de un modo legítimo".[22]

2.2.1. Límites a la recolección masiva de datos y a la vigilancia masiva

Para utilizar los sistemas de RFA, las fuerzas policiales deben contar con bases de referencia, es decir, las bases de información biométrica que van a usar para comparar las muestras obtenidas en los diferentes escenarios. Por ejemplo, pueden usar una base de plantillas faciales de reincidentes como base de referencia.

Un caso problemático se genera cuando, para cumplir sus cometidos, la policía inicia un proceso de recopilación masiva de datos biométricos o una migración de estos desde otro organismo gubernamental, incluyendo la información de toda la ciudadanía y sin su consentimiento. Esto contradice gravemente los principios de necesidad y proporcionalidad, aumenta notoriamente el riesgo de fuga de datos sensibles y trae al debate público la necesidad de buscar soluciones menos invasivas de la privacidad. Como principio general, los datos de personas inocentes no deben guardarse en bases de datos policiales o para fines de prevención criminal. Un Estado no debe tratar a todas las personas como criminales potenciales incluyéndolas en bases de datos de identificación facial con fines de vigilancia masiva.[23]

El RFA también se transforma en un método de vigilancia masiva, contraviniendo el principio legal de la presunción de inocencia, cuando el sistema de RFA es usado como medio de vigilancia en tiempo real en espacios públicos, ya sea eventual o permanente.

22 Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. «Informe sobre la vigilancia y los derechos humanos», A/HRC/41/35. (Asamblea General de las Naciones Unidas, 28 de mayo de 2019), accedido el 1 de febrero de 2022. https://www.undocs.org/es/A/HRC/41/35

23 La vigilancia masiva consiste en la vigilancia indiscriminada de un gran número de personas. Vulnera los principios de necesidad y proporcionalidad, así como el principio de presunción de inocencia.

Como principio general, los datos de personas inocentes no deben guardarse en bases de datos policiales o para fines de prevención criminal.

2.2.2. Supervisión y control democrático estricto

El uso policial de sistemas de RFA conlleva riesgos sobre derechos fundamentales, por lo que se necesita una adecuada regulación. Los diferentes escenarios de uso generan muchas preguntas. Por ejemplo: ¿bajo qué procedimiento una posible coincidencia de rostros desencadena un arresto?, ¿qué sucede en el caso de que una persona sea detectada erróneamente como sospechosa de un crimen debido a una falla en el algoritmo?, ¿quién decide cómo se calibra el sistema de RFA en cuanto a umbrales y puntajes de similitud?, ¿la policía puede vigilar preventivamente a cualquier persona en espacios públicos?, ¿la policía puede crear todas las listas de personas de especial interés que desee?, ¿quién decide la inclusión de un rostro asociado a un nombre en ese tipo de listas?. En definitiva, ¿cuál es exactamente el límite de las potestades de vigilancia policial?

El informe publicado por la International Network of Civil Liberties Organizations (INCLO) en enero de 2021[24] presenta una docena de casos que describen usos gubernamentales problemáticos de sistemas de RFA en el mundo. A continuación presentamos algunos de ellos:

- En 2018, un tribunal de apelaciones del Reino Unido determinó que el uso policial de RFA era ilegal, dado que violaba los derechos de privacidad y la ley de protección de datos. También encontró que esta tecnología discriminaba por motivos raciales o sexuales y que no había un marco legal suficiente para cumplir con la Convención Europea de Derechos Humanos (p. 7).
- Un residente de Detroit fue arrestado frente a su esposa y sus dos hijas en el año 2018 luego de que el sistema de RFA de la policía lo emparejó erróneamente con un ladrón de relojes. Esta persona fue retenida 30 horas antes de que se detectara el error. (p. 10)

24 INCLO (International Network of Civil Liberties Organizations), «In Focus. Facial Recognition Tech Stories and Rights Harms from Around the World», enero de 2021, https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf

- El uso de RFA por parte de las compañías de seguridad sudafricanas ha generado varios conflictos e instalado una nueva modalidad de apartheid basado en IA (p. 12).
- En Moscú, los participantes de manifestaciones antigubernamentales son incluidos en listas de seguimiento policial usando software de RFA. Ese mismo sistema se está utilizando actualmente para garantizar que las personas observen las reglas de cuarentena de covid-19 (p. 15).
- En 2019, la policía colombiana informó que se utilizarían helicópteros con sistemas de RFA para identificar a personas violentas durante las protestas contra el gobierno de Iván Duque, pero las organizaciones de la sociedad civil denunciaron que se utilizaban con el objetivo de disuadir la participación en manifestaciones pacíficas (p. 16).

En Argentina, la base de datos denominada "Sistema de Consulta Nacional de Rebeldías y Capturas" es usada para alimentar el sistema de RFA utilizado en el subterráneo de la ciudad de Buenos Aires. Un estudio reciente[25] detectó serios problemas de seguridad en el manejo de dicha base, que estaba desactualizada y que contenía varios errores, entre ellos la inclusión errónea de menores de edad. También se comprobó que existieron varias denuncias por detenciones ilegales debidas a falsos positivos[26] y a la ausencia de protocolos de uso.

Un aspecto a destacar cuando analizamos el tema de la supervisión y control del uso policial de sistemas de RFA es que, a pesar de que la mayoría de los países cuentan con leyes de protección de datos personales, la ciudadanía no siempre puede acudir a las autoridades nacionales de protección de datos para ejercer sus derechos. Esto sucede porque, en muchos países, el control del uso de las bases utilizadas en las actividades de seguridad pública e inteligencia no se encuentra dentro del alcance de los organismos de protección de datos.

25 Karen Hao, «Live Facial Recognition Is Tracking Kids Suspected of Being Criminals», MIT Technology Review, octubre de 2020. https://www.technologyreview.com/2020/10/09/1009992/live-facial-recognition-is-tracking-kids-suspected-of-crime/

26 «De un DNI mal cargado a una cara parecida: las víctimas del sistema de reconocimiento facial en Buenos Aires», *Todo Noticias*, 23 de julio de 2019, sec. Policiales. https://tn.com.ar/policiales/de-un-dni-mal-cargado-una-cara-parecida-las-victimas-del-sistema-de-reconocimiento-facial-en-buenos_980528/

Existe suficiente evidencia empírica que apoya las recomendaciones de los organismos de derechos humanos sobre la urgente necesidad de marcos legales específicos y transparentes para esta tecnología. Sin estos marcos, no existen garantías de que el sistema de RFA no sea objeto de un uso indebido o que arroje decisiones arbitrarias. Las políticas relacionadas con el uso de sistemas de IA por parte de los gobiernos deben asegurar la transparencia, participación ciudadana y rendición de cuentas en el desarrollo e implementación de estas soluciones.

> **Los Estados tienen "la obligación legal de prevenir la vigilancia masiva, que por definición no cumple con los principios de necesidad y proporcionalidad, y de prohibir las aplicaciones que puedan dar lugar a dicha vigilancia masiva".**
>
> Informe A9-0232/2021 Parlamento Europeo[27]

2.2.3. Amenaza al derecho a vivir una vida libre de discriminación

Como ya hemos visto, un sistema de RFA solo puede "reconocer" rostros dentro de los parámetros de los datos en los que ha sido entrenado y expuesto previamente. Si ciertos tipos de rostros (por ejemplo, rostros de personas afrodescendientes, asiáticas y de minorías étnicas, rostros femeninos, de personas con discapacidad —como el síndrome de down— o de la población LGBTQ) están subrepresentados en los conjuntos de datos de entrenamiento de RFA, entonces este sesgo se reflejará en el uso de la tecnología por parte de las personas que operan con ella.

Es por esto que el Estado debe brindar garantías contra los actos discriminatorios, exigir análisis de impacto obligatorios y públicos, y asegurar procesos de impugnación y revisión continua que incluyan la participación de la sociedad civil, especialmente de las poblaciones potencialmente afectadas.

27 Comisión de Libertades Civiles, Justicia y Asuntos de Interior, «Informe sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales», A9-0232/2021 (Parlamento Europeo), 13 de julio de 2021. https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_ES.html

2.3. Uso policial de RFA en el derecho comparado

A continuación se presentan dos ejemplos de normativa relacionada con el uso policial de sistemas de RFA.

- Una de nivel regional y de carácter programático: la Resolución A9-0232/2021 del Parlamento Europeo.
- Otra de nivel estatal y de carácter específico: Washington Senate Bill 6280 on Facial Recognition, en Estados Unidos.

2.3.1. Resolución A9-0232/2021 del Parlamento Europeo

En octubre de 2021, el Parlamento Europeo adopta la "Resolución sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales",[28] por la que solicita a los países la prohibición del reconocimiento facial automatizado (entre otros análisis biométricos) en espacios públicos. Además, recomienda considerar como de «alto riesgo» el uso de la identificación biométrica en el contexto de las actuaciones policiales y judiciales y, por lo tanto, que esté sujeto a requisitos adicionales.

A continuación citamos un extracto de la resolución:

> "25. Toma nota de los diferentes tipos de uso del reconocimiento facial, como, entre otros, la verificación/autenticación (es decir, la correspondencia entre una cara en vivo y una fotografía en un documento de identidad, por ejemplo, fronteras inteligentes), la identificación (es decir, la correspondencia de una foto con una base de datos de fotografías) y la detección (es decir, la detección de caras en tiempo real desde fuentes como las imágenes de CCTV y su correspondencia con bases de datos, por ejemplo, la vigilancia en tiempo real), cada una de las cuales tiene distintas implicaciones para la protección de los derechos fundamentales; cree firmemente que el despliegue de sistemas de

28 Parlamento Europeo, «Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales», A9-0232/2021. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.html

reconocimiento facial por parte de las autoridades policiales debe limitarse a fines claramente justificados y hacerse con pleno respeto de los principios de proporcionalidad y necesidad y de la legislación aplicable; reitera que, como mínimo, el uso de la tecnología de reconocimiento facial debe cumplir los requisitos de minimización de datos, exactitud de los datos, limitación del almacenamiento, seguridad de los datos y rendición de cuentas, además de ser legal, justo y transparente y perseguir un fin específico, explícito y legítimo que esté definido claramente en la legislación de los Estados miembros o la Unión; opina que los sistemas de verificación y autenticación solo pueden seguir desplegándose y utilizándose con éxito si sus efectos adversos pueden mitigarse y si se cumplen los criterios anteriores;

26. Pide, además, la prohibición permanente del uso de análisis automatizados o el reconocimiento en espacios accesibles al público de otras características humanas, como los andares, las huellas dactilares, el ADN, la voz y otras señales biométricas y de comportamiento;

27. Pide que se imponga una moratoria al despliegue de sistemas de reconocimiento facial para fines coercitivos con funciones de identificación, a menos que se utilicen estrictamente para fines de identificación de víctimas de delitos, hasta que las normas técnicas puedan considerarse plenamente acordes con los derechos fundamentales, los resultados obtenidos no estén sesgados y no sean discriminatorios, el marco jurídico prevea salvaguardias estrictas contra el uso indebido y un control y supervisión democráticos estrictos y existan pruebas empíricas de la necesidad y proporcionalidad del despliegue de estas tecnologías; señala que, cuando no se cumplan los criterios anteriores, los sistemas no deben utilizarse ni desplegarse."

2.3.2. Washington Senate Bill 6280 on Facial Recognition - Estados Unidos

En Estados Unidos, luego de la conmoción pública que generó el uso de RFA para la persecución de manifestantes en el marco de las protestas por el asesinato de George Floyd, conocidas empresas tecnológicas decidieron moratorias en la oferta de sus

soluciones de RFA a los gobiernos,[29] solicitando que su uso sea regulado de forma detallada por la vía parlamentaria. A su vez, en el año 2020, varios estados de Estados Unidos decidieron prohibir o regular el uso de RFA con fines de vigilancia policial.

Un ejemplo de regulación detallada y que incorpora mecanismos de salvaguarda es la Washington Senate Bill 6280 on Facial Recognition.[30] Si bien en junio de 2021 trascendió en la prensa que el Estado de Washington prohibió el reconocimiento facial con fines de vigilancia pública,[31] la realidad es que la Washington SB 6280 no prohíbe sino que regula el uso policial del RFA, limitándolo a ciertas circunstancias. De hecho, lo que se prohíbe es el uso de RFA para vigilancia en tiempo real o sostenido sin orden judicial y se limitan los supuestos en los que un juez está en condiciones de dar esa autorización.

A continuación, realizamos una breve descripción de los aspectos regulados por la Washington SB 6280.

La Sección 3 de dicha ley prevé que, antes de desarrollar o adquirir un software de RFA, cualquier organismo o agencia estatal debe dar noticia a la autoridad legislativa con un informe de rendición de cuentas que contenga, como mínimo:

1. El nombre del servicio de reconocimiento facial, proveedor y versión; y una descripción de sus capacidades y limitaciones generales.
2. El tipo o tipos de datos que utiliza como input la tecnología; cómo se generan, recopilan y procesan esos datos; y el tipo o tipos de datos que es razonablemente probable que el sistema genere.
3. Una descripción del propósito y el uso propuesto del servicio de reconocimiento facial; si se trata de un sistema de decisión final o de apoyo; y sus beneficios previstos, incluyendo cualquier dato o investigación que demuestre esos beneficios.

29 Larry Magid, «IBM, Microsoft And Amazon Not Letting Police Use Their Facial Recognition Technology», Forbes, 12 de junio de 2020. Accedido el 2 de febrero de 2022. https://www.forbes.com/sites/larrymagid/2020/06/12/ibm-microsoft-and-amazon-not-letting-police-use-their-facial-recognition-technology/

30 Senate of the State of Washington, «Chapter 43.386 RCW: Facial Recognition», Senate Bill 6280, Revised Code of Washington, accedido el 1 de febrero de 2022. https://app.leg.wa.gov/RCW/default.aspx?cite=43.386

31 «Washington State County Bans Use of Facial Recognition», US News & World Report, 2 de junio de 2021.https://www.usnews.com/news/best-states/washington/articles/2021-06-02/washington-state-county-bans-use-of-facial-recognition

4. Una política clara de uso y gestión de los datos, incluyendo protocolos específicos que cubran los siguientes aspectos:
    a. Cómo y cuándo se implementará o utilizará el servicio de reconocimiento facial y por quién, incluyendo los factores que se utilizarán para determinar la implementación de la tecnología, y otra información relevante, como si la tecnología se operará continuamente o se usará solo en circunstancias específicas. Si el servicio de reconocimiento facial será utilizado por otra entidad en nombre de la agencia, el informe de rendición de cuentas del servicio de reconocimiento facial debe incluir explícitamente una descripción del acceso de la otra entidad y cualquier protocolo aplicable.
    b. Cualquier medida tomada para minimizar la recopilación inadvertida de datos adicionales más allá de la cantidad necesaria para el propósito específico para el cual se utilizará el servicio de reconocimiento facial.
    c. La política de integridad y de retención de datos.
    d. Las medidas de seguridad de datos aplicables al servicio de reconocimiento facial, incluida la forma en que los datos recopilados mediante el servicio de reconocimiento facial se almacenarán y accederán de forma segura.
    e. La manera en la que el proveedor de servicios de reconocimiento facial procura cumplir con los requisitos de notificación de brechas de seguridad.
    f. Un plan de capacitación y la manera en la que la agencia se asegurará de que todo el personal que opere el servicio de reconocimiento facial o acceda a sus datos conozca y pueda garantizar el cumplimiento de la política de uso y administración de datos antes del uso del servicio de reconocimiento facial.
5. Los procedimientos de testeo periódico que se planifica realizar para el uso del sistema de RFA en condiciones no controladas.
6. Un análisis que describa el impacto potencial de la tecnología en las libertades civiles, las estadísticas de falsas coincidencias y cómo la agencia lidiará con esos errores (aunque sean menores al 1 % en pruebas en ambientes controlados).

En la Sección 4 se establece que, cuando una agencia gubernamental estatal o local utilice un servicio de reconocimiento facial para tomar decisiones que produzcan

efectos legales para las personas o efectos significativos similares, deberá asegurarse de que esas decisiones estén sujetas a una "revisión humana significativa". Este tipo de revisión se define como: "revisión o supervisión por parte de una o más personas capacitadas de acuerdo con la sección 7 de esta ley y que tienen la autoridad para modificar la decisión bajo revisión."

En la Sección 7 de la ley se plantean los requisitos mínimos de capacitación que deben cumplirse para formar al personal implicado directa e indirectamente en el uso del sistema.

La Sección 8 detalla los reportes anuales que deben realizar los jueces que han autorizado el uso de RFA y los reportes públicos que deben presentar las agencias, así como las auditorías a las que deben someterse estas.

La Sección 9 crea la "*Facial Recognition Task Force*", órgano integrado por miembros del parlamento y del gobierno, la sociedad civil, organismos de derechos humanos y la academia, encargado de dar seguimiento y realizar recomendaciones sobre el uso de RFA.

La Sección 11 establece la prohibición de usar un servicio de reconocimiento facial para desarrollar una vigilancia continua, realizar una identificación en tiempo real o casi en tiempo real, o iniciar un seguimiento persistente. Este tipo de vigilancia en tiempo real solo se podrá realizar mediante una orden judicial y únicamente con el propósito de localizar o identificar a una persona desaparecida o identificar a una persona fallecida. También establece requisitos y limitaciones para el uso de los resultados de RFA como medio de prueba judicial.

Finalmente, se establece que el uso de RFA en aeropuertos, puertos y licencias de conducir tendrá otro régimen.

3. El uso de RFA por la policía en Uruguay

3.1. Antecedentes

Desde el año 2010 y con el objetivo de mejorar la estrategia de trabajo para la prevención y disuasión del delito y el suministro de pruebas a la justicia, el Ministerio del Interior (MI) se ha embarcado en la instalación progresiva de sistemas de monitoreo y cámaras de videovigilancia en la vía pública. Actualmente existen casi 9 mil cámaras instaladas en todo el país.[32] Los sistemas de monitoreo forman parte del Sistema Integrado de Videovigilancia y Emergencia (SIVVE) que se encuentra a cargo del Centro de Comando Unificado (CCU). Este centro también se encarga del sistema de emergencias 911, de la Dirección de Monitoreo Electrónico (DIMOE), que opera el sistema de tobilleras electrónicas, y de la Dirección de Análisis Criminal.

En 2016, a propuesta de la Comisión Honoraria para la Prevención, Control y Erradicación de la Violencia en el Deporte, se creó el padrón de personas con antecedentes penales asociados a conductas de violencia en el deporte, a cargo del MI, y se estableció la obligación de las federaciones deportivas de contratar sistemas de control biométrico mediante RFA (Decreto 387/016).[33] Entre 2017 y 2018, la Asociación Uruguaya de Fútbol y la Federación Uruguaya de Basketball, asesoradas por el MI, comenzaron a instalar cámaras y sistemas de RFA para evitar el ingreso a sus espectáculos de las personas incluidas en el padrón de personas con antecedentes de violencia en el deporte. Las cámaras son operadas por funcionarios del MI. En el año 2018 había unas 500 personas incluidas en el padrón.[34]

Con la modificación realizada en 2020 de la Ley 19534 que regula el derecho de admisión y permanencia en espectáculos públicos,[35] y con su decreto reglamentario de

32 Ministerio del Interior, «La nueva policía: 10 años de videovigilancia», Ministerio del Interior - Noticias, 25 de octubre de 2019. https://www.minterior.gub.uy/index.php/unicom/noticias/7240-la-nueva-policia-10-anos-de-videovigilancia

33 Decreto N.° 387/016, «Medidas a aplicar en los eventos deportivos», disponible en: https://www.impo.com.uy/bases/decretos-originales/387-2016

34 Guillermo Losa, «Violencia: gobierno busca que el básquetbol siga mismo camino que el fútbol», El Observador, 13 de octubre de 2018, sec. Nacionales - Seguridad. https://www.elobservador.com.uy/nota/violencia-buscan-que-basquetbol-siga-mismo-camino-que-el-futbol-20181012205951

35 Ley N.° 19534, «Aprobación de la regulación del derecho de admisión y permanencia en espectáculos públicos», 2017. https://www.impo.com.uy/bases/leyes/19534-2017. La modificación se realizó mediante la Ley de Urgente Consideración N.° 19889 de 2020.

comienzos de 2021,[36] el uso de RFA en espectáculos deportivos pasa a tener un régimen más garantista. Esta nueva normativa deroga el decreto anterior y establece un marco detallado para el ahora denominado "registro de personas impedidas de ingresar a los espectáculos", así como para el ejercicio de los derechos de admisión y el derecho de exclusión en espectáculos. Se establecen criterios para la inclusión de personas en el registro, se detallan las causales y el procedimiento de ingreso y también se establecen las vías para solicitar la revisión de la sanción. Además, se determina una duración gradual de la permanencia en el registro en base a la gravedad de la conducta. Este registro pasa a estar a cargo de las federaciones deportivas, que deben comunicar los nombres al MI. En cuanto al uso de sistemas de RFA, se establece que pueden ser utilizados con fines de control de ingreso y, en general, para el apoyo al cumplimiento de los cometidos de la policía en eventos deportivos que el MI califique como de alto riesgo.

También en 2020, el Parlamento de Uruguay sancionó la Ley de Presupuesto.[37] Los artículos 191 y 192 de esta ley disponen la creación de una base de datos de identificación facial para su tratamiento con fines de seguridad pública a cargo de la Secretaría del MI. Esta base se crea copiando las fotografías y otros datos personales de personas mayores de edad de la base de la Dirección Nacional de Identificación Civil (DNIC), encargada de emitir la cédula de identidad y el pasaporte, y habilitando la migración de estos datos a los servidores de la Secretaría del MI.

Esta reforma legislativa era necesaria para habilitar a la policía a utilizar los datos de identificación facial de la DNIC como base de referencia en el software de RFA que ya había adquirido mediante una licitación pública que culminó en febrero de 2020.[38]

De forma paralela al avance del uso de RFA con fines de seguridad en Uruguay, tanto la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic) como la sociedad civil iniciaron procesos intentando contribuir al debate ciudadano sobre este tema.

36 Decreto N.° 01/021, «Reglamentación del art. 1 bis de la Ley 19534, relativa a la creación de un registro de personas impedidas de ingresar a espectáculos públicos», disponible en: https://www.impo.com.uy/bases/decretos/1-2021

37 Ley N.° 19924, «Presupuesto Nacional de Sueldos Gastos e Inversiones. Ejercicio 2020-2024», 2020. https://www.impo.com.uy/bases/leyes/19924-2020

38 Secretaría del Ministerio del Interior, «Licitación Pública 13/2019. Adquisición de una Plataforma de Identificación Facial, y servicio técnico de soporte, corrección, actualización y mantenimiento local (Pliego 744940)», Agencia Reguladora de Compras Estatales, agosto de 2018. https://www.comprasestatales.gub.uy/consultas/detalle/id/744940

En 2020, la Agesic define la "Estrategia de Inteligencia Artificial para el Gobierno Digital".[39] Esta estrategia comenzó con una consulta pública y abierta. Su objetivo general es promover y fortalecer el uso responsable de la IA en la administración pública, generando capacidades e impulsando la participación y confianza de la ciudadanía en el uso gubernamental de estos sistemas. Dentro de esta estrategia encontramos el "respeto de los derechos humanos" y la "transparencia" como dos de los principios fundamentales.

En 2021, el Laboratorio de Datos y Sociedad (Datysoc), con el apoyo de Amnistía Internacional Uruguay, DATA Uruguay, CAInfo y Ártica, presentaron la propuesta de "Mesas de diálogo sobre uso de sistemas de vigilancia automatizada" en el 5° Plan de Acción de Gobierno Abierto 2021-2025,[40] [41] como oportunidad para la aplicación de la estrategia de inteligencia artificial para el gobierno digital de la Agesic. Las organizaciones de la sociedad civil buscaban gestionar un compromiso por parte del MI que permitiera un debate informado y la participación de las múltiples partes interesadas para la reglamentación de los sistemas de vigilancia automatizada del Estado. Lamentablemente, no se logró un compromiso del MI para llevar a cabo esta propuesta.

3.2. Tipo de software adquirido y funcionalidades

Un consorcio integrado por las empresas DDBA Ltda, CDT LATAM LLC y TTY SA resultó adjudicatario de la licitación del MI para brindar una plataforma de RFA y servicios asociados. La solución se basa en el algoritmo de RFA del desarrollador Herta Security. El algoritmo de Herta Security se encuentra en el puesto número 266 de 385 en el ranking

39 «Estrategia de Inteligencia Artificial para el Gobierno Digital», Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, 2020. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial-para-gobierno-digital/estrategia

40 Datysoc (Laboratorio de Datos y Sociedad), «Mesas de Diálogo sobre Uso de Sistemas de Vigilancia Automatizada. (Código de la propuesta: GA-2021-05-24)», Consulta pública: 5to Plan de Acción Nacional de Gobierno Abierto - Plataforma de Participación Ciudadana Digital, 4 de mayo de 2021. https://quinto-plan.gobiernoabierto.gub.uy/proposals/24-mesas-de-dialogo-sobre-uso-de-sistemas-de-vigilancia-automatizada

41 Juan Pablo De Marco, «Cómo funciona el ciberpatrullaje y el reconocimiento facial: la mesa de diálogo solicitada al gobierno», El Observador, 7 de mayo de 2021, sec. Tecnología. https://www.elobservador.com.uy/nota/como-funciona-el-ciberpatrullaje-y-el-reconocimiento-facial-el-pedido-al-gobierno-20215618260

del NIST en cuanto a su desempeño en la función verificación de rostros (1 a 1) en ambientes no controlados[42] y no se encuentra rankeado en las pruebas de desempeño de identificación (1 a N) de dicho organismo.

El software se contrató por el término de tres años a partir de febrero de 2020, hasta febrero de 2023. Vencido el contrato, el Ministerio podrá solicitar a la empresa que el servicio se preste hasta la sustanciación del nuevo llamado.

El pliego preveía la realización de una serie de pruebas que el software de cada oferente debía superar. Como no fue posible acceder a los resultados de estas pruebas, a continuación se resume la información disponible en el Anexo II de especificaciones técnicas del pliego de licitación:[43]

- El MI entrega a los oferentes un set de 10 mil fotografías[44] que sirven de referencia y que deben ser previamente enroladas en el sistema, generando una plantilla para cada rostro.
- Luego, las plantillas generadas para ese set de 10 mil imágenes deben ser comparadas con otra base de 5 mil imágenes y videos cumpliendo con diferentes pruebas. El resultado de estas pruebas se entrega en un sobre cerrado.
- Pruebas de enrolamiento: se tolera únicamente una tasa de fallo en la inscripción de un 0,1 (únicamente 10 errores de enrolamiento en la base de 10 mil rostros)
- Pruebas de identificación: una de las pruebas de identificación es excluyente. En esta prueba, la tasa de errores de identificación (falsos negativos y falsos positivos) no debe superar el 10 %. Las otras pruebas de identificación no tienen requisitos mínimos.
- Pruebas de verificación: no se plantean requisitos mínimos excluyentes para las pruebas de verificación.

Vale la pena aclarar que, aún si el desempeño del software ganador de la licitación fue muy bueno, la superación de estas pruebas de funcionamiento:

42 Patrick Grother et al., «Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification», NIST, 24 de enero de 2022, p.37. https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf

43 Anexo II «Especificaciones técnicas». Licitación Pública 13/2019 (Pliego 744940). .https://www.comprasestatales.gub.uy/Aclaraciones/aclar_llamado_744940_0.ods

44 Las especificaciones técnicas del pliego establecen que estas imágenes fueron adquiridas de acuerdo a las especificaciones ICAO usadas para imágenes de pasaportes e identificación, garantizando un estándar mínimo de calidad.

- No garantiza el manejo y configuración correcta de los umbrales o la interpretación adecuada al contexto de los puntajes de similitud por parte del MI.
- No garantiza que no surjan problemas cuando el algoritmo sea usado en ambientes no controlados.
- No garantiza que no existan problemas de discriminación por sesgo.

3.3. Implementación del sistema y escenarios de uso

3.3.1. ¿Qué funcionalidades tiene el software contratado por la policía?

El anexo de especificaciones técnicas del pliego de licitación indica las funcionalidades mínimas que fueron requeridas a las empresas que se presentaron en la licitación. De esas funcionalidades se desprende que, con el software adquirido, será posible:

- *Crear plantillas faciales para cada persona mayor de edad*. El software debe procesar una base de datos biométrica de al menos cuatro millones de identidades que incluya a toda la población de Uruguay y movimientos migratorios de interés (Anexo II, Id 22). Esto implica el enrolamiento al sistema de RFA y la creación de plantillas faciales para cada ciudadano y ciudadana de Uruguay, así como para personas extranjeras a definir.
- *Ser utilizado en al menos 300 estaciones de trabajo de oficiales de caso* (Anexo II, Id 8). Esto implica el uso forense del sistema en diferentes estaciones del CCU.
- *Crear perfiles y listas de personas con diferentes fines*. El software debe ser capaz de armar y administrar listas globales de personas de interés y listas por unidad operativa del MI, así como mecanismos de configuración de alertas para dichas listas. También debe brindar la posibilidad de interoperar con listas de otros sistemas del Ministerio, por ejemplo, con listas de personas requeridas del Sistema de Gestión de Seguridad Pública[45] (Anexo II, Id 43, 44 y 45). Esto implica la posibilidad

45 El Sistema de Gestión de Seguridad Pública (SGSP) es una herramienta informática que gestiona la información de todas las unidades ejecutoras policiales de Uruguay. El sistema registra todos los procesos de gestión de eventos de seguridad pública que están documentados en la legislación vigente y tiene vocación de interoperabilidad con otros sistemas de uso policial, como el sistema de tobilleras de la DIMOE y el de videovigilancia del SIVVE, entre otros.

de crear perfiles y listas de personas con diferentes fines (por ejemplo, personas prófugas, desaparecidas, activistas, participantes en manifestaciones, etc.).

- *Montar un mecanismo de verificación/identificación facial para que usen los oficiales en el territorio*. Se prevé la posibilidad de dotar a 3 mil oficiales de policía con dispositivos móviles con una aplicación de RFA (Anexo II, Id 8). Esto implica su uso en la vía pública, probablemente con fines de confirmación de identidad.
- *Vigilar en tiempo real mediante streaming e identificación facial*. Se valora que el sistema sea capaz de procesar, puntualmente y a demanda, streaming de cámaras en vivo, para efectuar vigilancia en tiempo real mediante identificación facial (1 a N). Se sugiere a los oferentes del llamado cotizar una solución que permita una lista de búsqueda de 10.000 registros utilizando hasta 5 streamings simultáneos (Anexo II, Id 89). Esto implica la posibilidad de identificación facial en tiempo real en espacios públicos. Si bien este requisito no es excluyente en el pliego, informantes calificados nos confirman que la solución contratada cumple con esta funcionalidad.
- *Integrar el sistema de RFA con otros sistemas de gestión y vigilancia*. La solución contratada debe permitir integrar el sistema de reconocimiento facial con aplicaciones y sistemas propios o de terceros (Anexo II, Id 8, 48, 50, 63, 66). Esto incluye la integración con el sistema de videovigilancia del MI y con el SGSP (Anexo II, Id 43). También brinda amplias posibilidades de triangulación de datos con diferentes plataformas, por ejemplo, con Ucinet, software de ciberpatrullaje en redes sociales que el MI adquirió en 2020 y declaró estar testeando.[46]

Los usos descritos en este punto son usos potenciales que se derivan de la simple lectura de los requisitos mínimos del software que el pliego de licitación exigió cumplir a los oferentes. El MI aún no ha publicado información relativa al uso efectivo del sistema de RFA ni ha confirmado si se encuentra operativo.

46 «Ministerio del Interior adquirió un nuevo software que analiza las interacciones sociales para identificar grupos criminales», Semanario BUSQUEDA, 17 de marzo de 2021, sec. Información Nacional. https://www.busqueda.com.uy/Secciones/Ministerio-del-Interior-adquirio-un-nuevo-software-que-analiza-las-interacciones-sociales-para-identificar-grupos-criminales-uc46916

3.3.2. Información sobre el uso del sistema contratado

En agosto de 2021 realizamos entrevistas a informantes calificados a los efectos de obtener datos relacionados con el uso del sistema contratado. La información que se brinda a continuación no constituye información oficial avalada por el Ministerio del Interior.

Las personas entrevistadas informan que ya se realizó una copia de la base de la DNIC de la totalidad de las imágenes faciales de las personas mayores de edad, los nombres y apellidos de sus titulares, sexo, fecha de nacimiento, nacionalidad, número de cédula de identidad, fecha de expedición y fecha de expiración de la misma. Esta base se actualizará regularmente, aunque a la fecha de las entrevistas no existe un protocolo de actualización. La base se encuentra en el centro de datos de la Secretaría del MI. Las imágenes están siendo enroladas en el sistema.

En la fecha en que se tomaron las entrevistas, la implementación del sistema se encuentra en proceso y el MI está trabajando en el establecimiento de los escenarios de uso y en los protocolos de uso policial del software de RFA. Estas decisiones, de corte operativo, se toman en el CCU. De acuerdo con las personas entrevistadas, los casos de uso que se consideran como posibles son dos:

- El uso forense mediante verificación o identificación retrospectiva en estaciones de trabajo del CCU.
- La verificación o identificación mediante el uso de una app en tablets o móviles conectados a la red del MI y proporcionados a los efectivos policiales.

En cuanto a las especificaciones técnicas que se incluyeron al momento de dimensionar lo solicitado en el pliego de licitación y los usos potenciales descritos en el punto anterior, las personas entrevistadas aclaran que es común pedir más de lo que efectivamente se usará. Esto se hace para contratar la mejor solución pensando también en el largo plazo. A pesar de que la identificación en tiempo real en la vía pública es posible utilizando la herramienta contratada, para efectivizar ese uso será necesario contar con más presupuesto e inversiones.

Los casos de uso más probables a corto plazo son dos:

1. El uso forense mediante verificación o identificación retrospectiva.

2. La verificación o identificación mediante el uso de una app en tablets o móviles proporcionados a los efectivos policiales.

Van a existir protocolos, pero los protocolos de uso operativo policial no suelen ser públicos.

Existirán diferentes tipos de usuarios con diferentes roles y niveles de acceso al sistema. Las características de los perfiles de usuarios deberán ser definidos en los protocolos de uso. De cualquier forma, según los entrevistados, es muy seguro que existan al menos cuatro tipo de usuarios: 1) el administrador general del sistema, 2) un perfil de usuario avanzado con potestades para realizar búsquedas en el sistema, que sería desempeñado por un oficial del CCU que recibiría las solicitudes de comparación de rostros, 3) un perfil con permisos para realizar solicitudes al sistema cargando un video o una imagen, por ejemplo, un "oficial de caso" que trabaja junto con el fiscal y que desea realizar una solicitud de comparación, y por último, 4) un usuario auditor con potestades de control (este rol está previsto en la herramienta contratada).

En definitiva, nos informan que existirán protocolos, asignación de diferentes roles y responsabilidades dentro del sistema, así como trazabilidad de las consultas y eventos. Las personas entrevistadas expresan que los protocolos de uso operativo policial no suelen ser públicos.

En cuanto a las listas de personas de interés, se aclara que este concepto de lista es anterior al sistema de RFA. Estas listas se crean por orden judicial (por ejemplo, listas "negras" de personas requeridas por la justicia o impedidas de salir del país), o bien en el marco de los procesos de investigaciones (listas "grises"). Aún no está determinado cómo funcionará el sistema de listas en el marco del uso de RFA.

Consultadas sobre los aspectos de capacitación en el funcionamiento del sistema contratado, las personas entrevistadas expresaron que está previsto un proceso de instrucción.

Finalmente, en cuanto a los riesgos de sesgos y a las tasas de error de la herramienta contratada, las personas entrevistadas consideran que se contrató una solución con excelentes referencias. Expresan que la empresa declara que los datos de entrenamiento del algoritmo varían según la demografía de la región donde se ofrece la solución y garantiza paridad estadística entre hombres y mujeres, aunque la empresa no entrega la información sobre datos de entrenamiento.

3.4. Ausencia de base legal para el uso policial de RFA

No existe ninguna normativa específica que regule el uso del RFA por el Ministerio del Interior. Los artículos 191 y 192 de la Ley de Presupuesto de 2020 no tratan específicamente sobre RFA, sino que únicamente legalizan el uso policial de los datos biométricos de identificación facial de la DNIC. A su vez, estos artículos otorgan al MI una amplia discrecionalidad en cuanto a qué uso se le dará a la base de identificación facial, habilitando una inmensa base de referencia, con los datos de toda la ciudadanía, para realizar enrolamientos masivos en sistemas de RFA contratados.

Artículo 191

Créase en el Inciso 04 "Ministerio del Interior", Unidad Ejecutora 001 "Secretaría del Ministerio del Interior", una base de datos de identificación facial para su administración y tratamiento con fines de seguridad pública, en estricto cumplimiento de los cometidos asignados por la Ley N.º 19315, de 18 de febrero de 2015, y a lo dispuesto en la Ley N.º 18331, de 11 de agosto de 2008.

Artículo 192

Autorízase en el Inciso 04 "Ministerio del Interior", Unidad Ejecutora 031 "Dirección Nacional de Identificación Civil", la migración actualizada a la Unidad Ejecutora 001 "Secretaría del Ministerio del Interior", de la totalidad de las imágenes faciales de las personas mayores de edad de las que lleva registro, los nombres y apellidos de sus titulares, sexo, fecha de nacimiento, nacionalidad, número de cédula de identidad, fecha de expedición y fecha de expiración de esta última.

El artículo 191 enmarca el uso de los datos de identificación facial al estricto cumplimiento de los cometidos de la Ley Orgánica Policial (Ley 19315). Los artículos 4 y 5 de la Ley Orgánica Policial[47] establecen estos cometidos mediante expresiones tales como "hacer cumplir las leyes" o "prevenir la comisión de delitos" o "investigar los delitos o hechos con apariencia de delito". Estas expresiones genéricas definitivamente no aportan un marco regulatorio específico con pautas o garantías mínimas.

Otra normativa aplicable al uso policial de sistemas de RFA es la Ley 19696 que regula el Sistema Nacional de Inteligencia.[48] Esta ley define como inteligencia policial a la "actividad que comprende lo relativo a la obtención, procesamiento, análisis y distribución de información relativa a la prevención y eventual represión del delito común y el crimen organizado en su calidad de auxiliar de la Justicia, a través de la prevención y represión del delito" (artículo 3, literal E). La misma ley, en su artículo 5, plantea los principios a los que deberán ajustar su actuación los integrantes del Sistema Nacional de Inteligencia. Entre estos principios se establece el principio de juridicidad, que "refiere a la estricta observancia de la Constitución, los tratados internacionales, las leyes y demás fuentes del ordenamiento jurídico, evitando en todo caso las actividades invasivas de la privacidad de las personas." (artículo 5, literal D). La Ley de Inteligencia plantea principios generales pero tampoco aporta elementos suficientes para evaluar la compatibilidad del marco de acción policial en torno al RFA con respecto al marco internacional de los derechos humanos.

La policía posee amplia discrecionalidad para decidir si restringe el uso del RFA a fines estrictamente forenses, como la verificación o identificación de un sospechoso a partir de una imagen estática, o si decide su uso con fines de inteligencia para la prevención de delitos mediante vigilancia en tiempo real en redes sociales o en espacios públicos. Ambos serían usos compatibles con los cometidos de la Ley Orgánica Policial y con la ley que regula el Sistema Nacional de Inteligencia. Los usos que hace la policía actualmente no se encuentran sometidos a ninguna supervisión, mecanismo de auditoría externa o rendición de cuentas.

47 Ley N.° 19315, «Aprobación de la Ley Orgánica Policial», 2015. https://www.impo.com.uy/bases/leyes/19315-2015

48 Ley N.° 19696, «Aprobación y regulación del Sistema Nacional de Inteligencia del Estado», 2018. https://www.impo.com.uy/bases/leyes/19696-2018

En definitiva, no existe un marco jurídico específico aplicable, por lo que queda en manos de la fuerza policial determinar cuándo persigue un "objetivo legítimo" y cuándo una actividad es "invasiva de la privacidad de las personas", así como decidir sobre los aspectos de necesidad y proporcionalidad.

3.5. Vacíos en el régimen de protección de datos personales (Ley 18331)

El artículo 191 de la Ley de Presupuesto de 2020 también enmarca el uso de la base de datos de identificación facial al estricto cumplimiento de las disposiciones de la Ley de Protección de Datos Personales (Ley 18331).[49] A continuación analizaremos cuáles serían las disposiciones aplicables.

3.5.1. Excepciones para bases de datos destinadas a seguridad pública

El artículo 3 de la Ley de Protección de Datos Personales deja fuera del ámbito objetivo de esta ley a las bases "que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito."

Consultado para esta investigación sobre el alcance de esta excepción, el Consejo Ejecutivo de la URCDP expresa:

> "Con carácter general, de acuerdo con el artículo 3° literal b) de la Ley N.° 18331 de 11 de agosto de 2008, las bases de datos que tienen como objeto la seguridad pública se encuentran excepcionadas de la aplicación de esta normativa. En el caso del Ministerio del Interior por tanto, aquellas bases de datos que tengan esta finalidad, no están alcanzadas por las obligaciones que establece esta normativa.
>
> No obstante, cabe indicar que, aun en los casos indicados en el párrafo anterior, se ha interpretado por parte de la URCDP que igualmente resultan aplicables con carácter general los principios de la protección de datos personales.

49 Ley N.° 18331, «Ley de Protección de Datos Personales», 2008. https://www.impo.com.uy/bases/leyes/18331-2008

> Esta excepción se complementa con lo previsto en el artículo 25 de la citada Ley N.° 18331, que indica que quedan sujetos a ésta, los datos personales que, por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en las bases de datos de los organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichas bases de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales."

En definitiva, el MI se encuentra sujeto a la Ley de Protección de Datos Personales con estas particularidades:

- Cuando se trate de bases de datos del MI que no tengan como finalidad la seguridad pública (por ejemplo, las bases de datos de funcionarios o proveedores, entre otras), el MI debe cumplir con la normativa de protección de datos, incluyendo las obligaciones formales previstas en la ley.
- Cuando se trate de bases de datos del MI cuya finalidad sea la seguridad pública, el MI debe cumplir de forma genérica con los principios de legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva y responsabilidad, por tratarse la protección de datos de un derecho fundamental. Pero, en este caso, las bases quedan fuera del control de la URCDP y no se requiere cumplir con las obligaciones formales previstas en la Ley 18331. Dentro de las obligaciones formales previstas en la Ley 18331 y en el Decreto 64/020[50] (esto es, aquellas que el MI no tiene obligación de cumplir), encontramos la obligación de registrar las bases, garantizar los derechos de acceso, rectificación y cancelación de datos, comunicar a la URCDP las vulneraciones de seguridad de datos dentro de un plazo de 72 horas, comunicar a la URCDP los resultados de evaluaciones de impacto en el tratamiento de datos que impliquen riesgos potenciales, entre otras.

50 Decreto N.° 64/020, «Reglamentación de los arts. 37 a 40 de la Ley 19670 y art. 12 de la Ley 18331, referente a protección de datos personales», 2020. https://www.impo.com.uy/bases/decretos/64-2020

Volviendo al RFA y a la base de identificación facial, el artículo 191 de la Ley de Presupuesto de 2020 establece expresamente que esta base de datos de identificación facial se crea para su administración y tratamiento con fines de seguridad pública. De esta forma, el MI cumple con el principio de legalidad[51] previsto en la Ley 18331 y se crea una base que puede operar fuera del control de la URCDP. Para este caso particular, el Consejo Ejecutivo de la URCDP aclara que el artículo 25 de la Ley 18331 "indica que el concepto de seguridad pública queda limitado a aquellos supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas. Por tanto, se debe estar a este criterio restrictivo para identificar cuáles bases de datos quedan excepcionadas." Volvemos entonces al mismo problema de falta de garantías y especificidad detectado en el punto anterior, ya que no existe normativa que permita definir cuándo el Ministerio actúa en "estricto cumplimiento de las misiones legalmente asignadas", más allá de las expresiones genéricas expresadas en los artículos 4 y 5 de la Ley Orgánica Policial.

Finalmente, en lo pertinente a la base de identificación facial creada en el ámbito de la Secretaría del MI, es importante resaltar que:

- El MI no estaría obligado a poner en conocimiento de la URCDP los resultados de las evaluaciones de impacto que se realicen en el caso de que de ellas resulte un riesgo potencial y significativo para los derechos de las personas titulares de los datos (artículo 7 del Decreto 64/020).
- No sería aplicable la normativa vigente sobre protección de datos personales para la grabación, conservación o almacenamiento de imágenes que se utilicen como base de comparación en el sistema de RFA, siempre que su tratamiento se realice con fines de seguridad pública. Por ejemplo, el MI no tiene obligación de informar públicamente dónde instalará zonas de videovigilancia ni cuándo está captando imágenes de la ciudadanía con dichas cámaras. Sin embargo, sí tiene la obligación de eliminar los datos personales registrados con fines policiales cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento (artículo 25 de la Ley 18331).

51 El artículo 9 de la ley 18331 establece que no es necesario el previo consentimiento cuando los datos se recaban para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

3.5.2. Incumplimiento de obligaciones formales de protección de datos personales

Como hemos visto, el MI se encuentra alcanzado por todas las obligaciones de la Ley de Protección de Datos Personales en lo que respecta al tratamiento de sus bases de datos que no tengan como finalidad la seguridad pública. De esta forma, el MI debe registrar sus bases almacenadas con fines administrativos en el registro de la URCDP y cumplir con la obligación de designar un delegado de protección de datos personales.[52] Consultada la URCDP sobre el cumplimiento de estas dos obligaciones, informa que, al mes de julio de 2021, "'la Secretaría del Ministerio del Interior' no ha registrado bases en el Registro que lleva adelante esta Unidad ni ha comunicado su delegado de protección de datos personales" (se adjunta en el anexo la respuesta de la URCDP a la solicitud de acceso a la información pública elevada ante ella).

La URCDP también informa que han tenido contacto con el MI ya que "dentro de los cometidos de la Unidad se encuentra asesorar a todos aquellos que así lo requieren (art. 34 de la Ley 18331). Especialmente se trabaja con todas las Entidades Públicas para que adecuen sus procesos internos a la normativa de protección de datos personales y en ese marco se han mantenido contactos con el Ministerio del Interior".

3.6. Falta de transparencia y de rendición de cuentas

Comprendiendo que la implementación del sistema de RFA se encontraba en proceso, decidimos esperar un tiempo prudencial antes de solicitar nueva información al MI. Esperamos hasta el mes de noviembre de 2021 para elevar una solicitud de acceso a la información pública con fines de seguimiento (se adjunta la solicitud de acceso en el anexo).

En diciembre de 2021, ya vencido el plazo legal de respuesta, el MI niega el acceso

52 De acuerdo con los artículos 10 y 11 del Decreto N.° 64/020, todas las entidades públicas deben designar un delegado de protección de datos personales, cuyas funciones principales son:
a) Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales.
b) Supervisar el cumplimiento de la normativa sobre dicha protección en la entidad o entidades para las que preste servicios.
c) Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en materia de protección de datos personales y verificar su realización.
d) Actuar como nexo entre su entidad y la Unidad Reguladora y de Control de Datos Personales.

a la información solicitada bajo el fundamento de que fue calificada como reservada de acuerdo con las resoluciones ministeriales Nº 5909/012[53] y Nº 5905/012[54] (se adjunta la respuesta a la solicitud de acceso en el anexo). De acuerdo con Jackson,[55] estas resoluciones forman parte de una serie de ocho resoluciones que el MI dictó en 2012, en las que se reservan genéricamente todo tipo de datos referentes al organismo, contraviniendo los estándares internacionales en materia de acceso a la información pública.

En particular, se entiende que esta denegatoria de información por parte del MI es de dudosa legalidad por los siguiente motivos:

- Si bien el artículo 9 de la Ley de Acceso a la Información Pública (Ley 18381) habilita al MI a clasificar la información como reservada, la misma ley, en su artículo 8, expresa que las excepciones al derecho de acceso a la información pública son de interpretación estricta.
- El Decreto 232/010 reglamentario de la Ley 18381 establece que el MI debe probar el daño contra un interés legítimo de la seguridad pública para clasificar la información como reservada,[56] requisito que está de acuerdo con los estándares básicos contenidos en los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información,[57] por lo que toda información que no afecte la seguridad pública deberá ser proporcionada.
- El Dictamen 17/013 de la Unidad de Acceso a la Información Pública analiza las ocho resoluciones de clasificación realizadas por el MI en el año 2012 (entre ellas, la

53 Ministerio del Interior, «Resolución N.º 5909», 30 de julio de 2012, https://www.minterior.gub.uy/images/stories/5909.pdf

54 Ministerio del Interior, «Resolución N.º 5905», 25 de julio de 2012, https://www.minterior.gub.uy/images/stories/5905.pdf

55 Matías Jackson, «Informe Acceso a La Información Pública Y Seguridad Nacional En Uruguay (Report on Access to Public Information and National Security in Uruguay)», SSRN Scholarly Paper, Rochester, NY: Social Science Research Network, 5 de julio de 2015, p. 12. https://doi.org/10.2139/ssrn.3514005

56 Decreto 232/010, «Reglamentación de la ley sobre el derecho de acceso a la información pública», 2010, art. 25. https://www.impo.com.uy/bases/decretos/232-2010

57 Estos principios fueron aprobados en octubre de 1995 por un grupo de personas expertas en derecho internacional, seguridad nacional y derechos humanos convocado por la organización Artículo 19 en colaboración con el Centro de Estudios Legales Aplicados de la Universidad de Witwatersrand, en Johannesburgo. Los principios constituyen requisitos estrictos que se requieren para limitar las libertades de opinión, expresión e información por razones de seguridad nacional. Se encuentran disponibles en: https://www.corteidh.or.cr/tablas/a22440.pdf

5909/012 y la 5905/012) y expresa que “no constituyen actos de clasificación propiamente dichos debido a su generalidad”. Sin embargo, el MI ha desconocido este dictamen y continuó utilizando estas resoluciones como fundamento sin probar el daño efectivo al interés tutelado que sería causado en cada caso concreto.

Las resoluciones del Ministerio del Interior que clasifican la información como reservada de forma genérica, abarcativa y sin probar el daño al interés público resultan en una denegación abusiva de información.

Lamentablemente, este manejo abusivo de la reserva de información no es un caso aislado sino una práctica sostenida por parte del MI que viene siendo denunciada sistemáticamente por la sociedad civil organizada.[58] Podemos nombrar varios ejemplos directamente relacionados con la seguridad informática y con la adquisición y uso de tecnologías de vigilancia:

- En 2015, el MI declaró como reservada toda la información relacionada con la adquisición del software de vigilancia de las comunicaciones “El Guardián” y se negaron las solicitudes de acceso a la información pública presentadas por DATA Uruguay y CAinfo.[59]
- El MI nunca respondió la solicitud de acceso a la información pública realizada por investigadores de la Web Foundation en el año 2017[60] para conocer aspectos técnicos de Predpol, software basado en IA que se utilizó para decidir dónde desplegar recursos de patrullaje. Estos investigadores expresan: “Por tanto, a la utilización de bases de datos secretas se suma la decisión de ocultar el diseño. De este modo PredPol se convierte en una caja negra, donde para las poblaciones

58 Ob. cit. nota 55, p. 12 y 13.

59 Scrollini, F. «Penumbra: Surveillance, security and public information in Uruguay». En «Global Information Society Watch 2014: Communications surveillance in the digital age». Association for Progressive Communications (APC) & Humanist Institute for Cooperation with Developing Countries (Hivos), 2014. https://giswatch.org/en/country-report/communications-surveillance/uruguay

60 Juan Ortiz Freuler y Carlos Iglesias, «Algoritmos e Inteligencia Artificial en Latinoamérica: Un Estudio de implementaciones por parte de Gobiernos en Argentina y Uruguay». World Wide Web Foundation, 2018. https://webfoundation.org/docs/2018/09/WF_AI-in-LA_Report_Spanish_Screen_AW.pdf

afectadas se vuelve imposible entender por qué se observa presencia policial en su cuadra con cierta regularidad." (p.28).

- En 2020, el MI rechazó el pedido de acceso a la información pública realizado por Gustavo Gómez (presidente de OBSERVACOM), en el que solicitó conocer si el MI monitorea las redes sociales para detectar amenazas y expresiones de odio.[61]
- El MI nunca respondió el pedido de informes parlamentario elevado en marzo de 2021 por la senadora Silvia Nane en torno al hackeo de las bases de datos de la DNIC. En entrevista a la senadora, ella informa que esta solicitud fue reiterada en el mes de junio y que el Senado la hizo suya el 6 de julio del mismo año. La senadora proporciona el texto del pedido de informes (ver anexo).

En resumen:

1. no existe un marco regulatorio que establezca los protocolos de acción, supervisión o auditoría externa sobre el uso del sistema de RFA,
2. la URCDP no tiene potestades de supervisión sobre las bases cuyo objeto sea la seguridad pública,
3. el MI no contesta o rechaza las solicitudes de acceso a la información pública, y
4. tampoco responde las solicitudes de informe parlamentario relacionadas con vulneraciones de seguridad a sus sistemas.

Las declaraciones del ministro del interior Luis Alberto Heber ante la Comisión Especial de Seguridad Pública y Convivencia de la Cámara de Senadores en julio de 2021 han elevado aún más las alarmas de la sociedad civil.[62] En dicha ocasión, la senadora Nane le recuerda la falta de respuesta al pedido de informe parlamentario sobre el hackeo de las bases de la DNIC y solicita que aporte información al respecto. Por su parte, el ministro expresa su preocupación ante la falta de inversión en seguridad informática por parte del MI y expresa voluntad de realizar fuertes inversiones en este sentido, sin aportar más información. A pesar de reconocer que urgen mejoras de inversión de seguridad

61 Ver: https://twitter.com/gusgomezgermano/status/1311650905134166017

62 Datysoc, «Vigilancia indiscriminada: dos propuestas preocupantes del Ministerio del Interior», Datysoc (blog), 21 de julio de 2021. https://datysoc.org/2021/07/21/vigilancia-indiscriminada-dos-propuestas-preocupantes-del-ministerio-del-interior/

informática, el ministro anuncia ante esta misma Comisión que existe la intención de crear nuevas bases de datos masivas, específicamente una base con el ADN de toda la ciudadanía, y de contratar un nuevo sistema de intercepción de comunicaciones cuando el presupuesto lo permita, ya que el actual sistema "El Guardián" resulta insuficiente.

3.7. RFA como medio de prueba

El uso como medio de prueba en procesos judiciales de los reportes resultantes del sistema de RFA contratado por la policía, presenta desafíos en términos de admisibilidad, valoración y garantías procesales.

La admisibilidad o inadmisibilidad como medio de prueba de un *match* que verifica o identifica a una persona depende de cómo se obtuvo la imagen o video que fue contrastada en el sistema de RFA.[63] Se deberá tomar en cuenta, para determinar si estas imágenes o videos fueron obtenidas legal o ilegalmente, lo dispuesto en la Resolución 58/021 del Consejo Ejecutivo de la URCDP en referencia al uso de cámaras de videovigilancia en diversos ambientes[64] y, especialmente para el ámbito penal, lo dispuesto en el artículo 210 de la Sección de Videovigilancia del Código del Proceso Penal.[65]

Resulta totalmente indispensable, para la correcta valoración de los reportes de RFA como medio de prueba, establecer un sistema de capacitación adecuada de todos los actores del sistema judicial y policial.

63 Camila Umpiérrez Blengio, «Admisibilidad de las grabaciones sin el consentimiento de quien participa y su divulgación», Revista Derecho Público, n.° 57, 14 de septiembre de 2020), p. 228 a 244. https://doi.org/10.31672/57.14

64 Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales, «Resolución N.° 58/021. Sobre el uso de cámaras de videovigilancia en diversos ambientes.», 21 de diciembre de 2021. https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-58021

65 Ley N.° 19293, «Código del Proceso Penal», 2014, artículo 210:
"210.1 El fiscal con noticia al juez y sin conocimiento del afectado, puede ordenar:
a) realizar tomas fotográficas y registro de imágenes;
b) utilizar otros medios técnicos especiales en lugares abiertos expuestos al público.
210.2 Se requerirá autorización judicial cuando dichas actividades se realicen en el interior de inmuebles o lugares cerrados." https://www.impo.com.uy/bases/leyes/19293-2014

4. Conclusiones

El uso de nuevas tecnologías por parte de los gobiernos implica nuevos enfoques y formas de vincularse con la ciudadanía. Al momento de evaluar la adquisición y las políticas de uso de sistemas de RFA, la policía no solo debe realizar una evaluación utilitarista en términos de efectividad y cumplimiento de los objetivos policiales. Ortiz Freuler e Iglesias expresan que la evaluación en términos de efectividad debe realizarse conjuntamente con el análisis de la legitimidad. La legitimidad no es sinónimo de legalidad, aunque la supone. Para determinar si el uso del sistema de RFA es legítimo, corresponde evaluar su legalidad, pero también observar tanto la legitimidad del proceso (participación de las poblaciones afectadas en el diseño de la política, explicabilidad de su funcionamiento, trazabilidad de responsabilidades) como la legitimidad en sus resultados (justos y no discriminatorios).[66]

> **Las políticas de uso de RFA deben tener en cuenta tanto la efectividad del sistema para analizar y resolver problemas, como la legitimidad del sistema en el proceso y en los resultados.**
>
> Freuler e Iglesias, 2018

Un llamado a la acción

Resulta preocupante la actual situación de inseguridad jurídica y opacidad en torno al uso policial de RFA en Uruguay. Es inaceptable la posibilidad actual y futura de que se someta a la ciudadanía a procesos de vigilancia masiva y a controles continuos de identidad, erosionando sus derechos fundamentales a la privacidad y la libertad de expresión.

Urge tomar medidas para asegurar que esto no ocurra, antes de que el sistema de RFA pase a la fase operativa (si es que aún se encuentra en la fase de pruebas). Algunas de las medidas urgentes a tomar son:

66 Ob.cit. nota 60, p. 6 y 7.

- **Prohibir el enrolamiento masivo de toda la población en el sistema de RFA.** Los artículos 191 y 192 de la Ley de Presupuesto de 2020 deberían derogarse y sustituirse por un régimen que cumpla con estándares básicos de derechos humanos.
- **Prohibir el uso de RFA como medio de vigilancia policial continua y sin orden judicial en espacios públicos.** De acuerdo con la información proporcionada por informantes calificados, el Ministerio del Interior debería realizar aún más inversiones para efectuar vigilancia en tiempo real mediante streaming de cámaras en vivo e identificación facial. Este argumento no debe ser utilizado como excusa para postergar la discusión. Todo indica que, de contar con el presupuesto necesario, existe intención de ir por este camino.
- **Sancionar una regulación adecuada y protocolos de actuación públicos,** que incluyan, al menos, la especificación detallada de los fines y escenarios de uso habilitados, los mecanismos de asignación de responsabilidad, las medidas para minimizar la recolección y retención de datos, así como los mecanismos de supervisión y transparencia adecuados.
- **Establecer mecanismos obligatorios de análisis de impacto y de evaluación de riesgo.** No existen registros públicos de la realización de análisis de impacto social y sobre los derechos humanos antes de la implementación del sistema de RFA. Esta información fue solicitada y no fue proporcionada. Algunas herramientas para realizar este tipo de análisis ya han sido desarrolladas por la URCDP, como por ejemplo la "Guía de evaluación de impacto en la protección de datos",[67] que facilita la detección de usos y escenarios de alto, mediano y bajo riesgo para la privacidad, así como estrategias de mitigación de daños.
- **Crear un programa de capacitación sobre funcionamiento y riesgos.** Específicamente, es apropiado determinar los diferentes tipos de usuarios del sistema (operadores, funcionarios policiales, actores del sistema de justicia, etc.) y exigir a cada usuario que complete un programa de capacitación. Dicha formación debería incluir alfabetización básica sobre el funcionamiento del sistema de RFA e

67 URCDP Uruguay y AAIP Argentina, «Guía de Evaluación de Impacto en la Protección de Datos», Unidad Reguladora y de Control de Datos Personales, 28 de enero de 2020, https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos

información sobre calibración de umbrales del sistema, así como otros aspectos técnicos relativos a los factores que influyen en la valoración de la precisión del sistema y los riesgos asociados.

- **Participación ciudadana antes de implementar el sistema de RFA.** Los funcionarios públicos encargados de tomar las decisiones clave pueden contar con información limitada o sesgada, lo que hace necesario detectar qué actores juegan un papel determinante en el impacto que tendrá el sistema. A pesar de que no prosperó la propuesta de "Mesas de Diálogo sobre Uso de Sistemas de Vigilancia Automatizada" presentada por organizaciones de la sociedad civil en el 5to Plan de Gobierno Abierto, sí se aprobó la propuesta de "Observatorio de Inteligencia Artificial en el Estado"[68] presentada por la Agesic. La creación de este observatorio constituye una oportunidad para establecer canales de participación ciudadana e instancias de debate.
- **Impulsar procesos de transparencia y rendición de cuentas.** La información relativa a la implementación del sistema de RFA debe ser pública y estar sujeta a un protocolo de supervisión externa por parte de la Suprema Corte de Justicia o de un órgano supervisor *ad hoc*. Este es un aspecto clave para lograr mayor confianza y legitimidad en la actividad policial. La información que deba permanecer reservada, por comprometer cuestiones operativas relacionadas con la seguridad pública o la lucha contra el crimen, debería detallarse especialmente, probando el daño a la seguridad pública, y no indicarse de forma genérica, de acuerdo con lo establecido en los artículos 8 y 9 de la Ley de Acceso a la Información Pública y el artículo 25 de su decreto reglamentario. En definitiva, se debe trabajar para aumentar la transparencia y la rendición de cuentas en la cultura institucional del MI, con el fin de adecuarla a los estándares internacionales en la materia.

68 Agesic, «Observatorio de Inteligencia Artificial en el Estado. (Código de la propuesta: PC-PROP-2021-11-116)», Consulta pública: 5to Plan de Acción Nacional de Gobierno Abierto - Plataforma de Participación Ciudadana Digital, 19 de noviembre de 2021. https://plataformaparticipacionciudadana.gub.uy/processes/quinto-planGA/f/17/proposals/116

Anexo documental

- Entrevista por escrito al Consejo Ejecutivo de la URCDP. Octubre de 2021. https://datysoc.org/wp-content/uploads/2022/02/Entrevista-por-escrito-al-Consejo-Ejecutivo-de-la-URCDP.pdf
- Pedido de informes parlamentario de la senadora Silvia Nane en torno al hackeo de las bases de datos de la DNIC. 4 de marzo de 2021. https://datysoc.org/wp-content/uploads/2022/02/Pedido-de-informes-parlamentario-Senadora-Nane-MINT-20210304-DNIC-Hackeo.pdf
- Solicitud de acceso a la información pública realizada ante la URCDP. 21 de junio de 2021. https://datysoc.org/wp-content/uploads/2022/03/Solicitud-de-acceso-a-la-informacion-publica-URCDP-21-6-2021.pdf
- Respuesta a la solicitud de acceso a la información pública realizada ante la URCDP. Resolución N.º 29-2021. 13 de julio de 2021. https://datysoc.org/wp-content/uploads/2022/02/Respuesta-a-la-solicitud-de-acceso-a-la-informacion-a-la-URCDP-Res-29-2021.pdf
- Solicitud de acceso a la información pública realizada ante el Ministerio del Interior. 1 de noviembre de 2021. https://datysoc.org/wp-content/uploads/2022/03/Solicitud-de-Acceso-a-la-Informacion-Publica-al-Ministerio-del-Interior-1-11-2021.pdf
- Resolución del Ministerio del Interior rechazando la solicitud de acceso a la información pública. Expediente N.º 2021-4-1-0007031. 2 de diciembre de 2021. https://datysoc.org/wp-content/uploads/2022/02/Resolucion-del-Ministerio-del-Interior-rechazando-la-solicitud-de-acceso-2-12-2021.pdf

Datysoc

LABORATORIO DE
DATOS Y SOCIEDAD