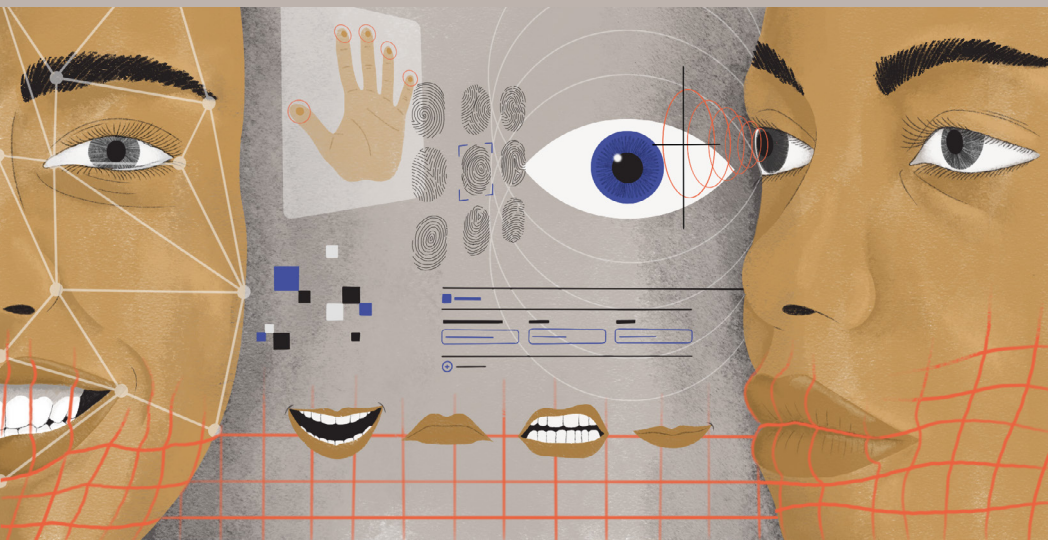


## LOS PRINCIPIOS

# Ojo con la Vigilancia. Cómo frenar el uso policial del reconocimiento facial

Principios para mitigar los daños a los derechos humanos de los sistemas de reconocimiento facial.



# INCLO



## Principios de INCLO sobre el uso de Sistemas de Reconocimiento Facial (SRF) por las fuerzas de seguridad

Nuestros principios señalan los estándares mínimos a seguir para la responsabilidad y mitigación de los daños que se derivan del uso de sistemas de reconocimiento facial, pero no respaldan el uso de los mismos por la policía. Constituyen una herramienta para construir consenso sobre los graves riesgos que se derivan del uso SRF y la necesidad urgente de severas restricciones o prohibiciones completas.

Estos principios se diseñaron para abordar:

- El uso directo de SRF por las fuerzas de seguridad;
- Cualquier uso de SRF para las fuerzas de seguridad llevado a cabo por una autoridad de otra jurisdicción; y
- Cualquier uso de SRF para las fuerzas de seguridad realizado por un tercero.

## **LOS PRINCIPIOS**

1. Las autoridades de las fuerzas de seguridad no deben usar SRF sin una base jurídica específica.
2. Las evaluaciones de impacto en derechos fundamentales deben ser obligatorias.
3. Las evaluaciones de impacto en derechos fundamentales deben ser independientes de las evaluaciones realizadas por proveedores.
4. No debe adquirirse ni desplegarse ningún sistema nuevo sin una garantía de independencia futura respecto de los proveedores.
5. Todas las versiones de todas las evaluaciones deben hacerse públicas antes del despliegue de un sistema.
6. La consulta pública sobre el despliegue de SRF debe ser obligatoria.
7. Las autoridades deben informar al público cómo se usan las imágenes de consulta en las operaciones de un sistema.
8. Los requisitos técnicos de cualquier sistema de reconocimiento facial deben ser de conocimiento público antes de su despliegue.
9. Los SRF en vivo están prohibidos.
10. La autorización judicial previa al uso de SRF debe ser obligatoria.
11. Las autoridades deben documentar cada búsqueda de SRF retrospectivos o iniciados por operador.
12. El resultado de un sistema, por sí solo, no es una base suficiente para interrogar, arrestar o detener.
13. Cuando un sistema de reconocimiento sea utilizado contra una persona, esta debe ser informada de los detalles del uso del mismo.
14. Cualquier identificación errónea causada por un sistema de reconocimiento facial debe ser informada.
15. Los informes anuales de las autoridades sobre identificaciones erróneas deben ser obligatorios.

16. Se debe establecer un organismo independiente de control de SRF antes de cualquier uso de uno de estos sistemas.
17. Ese organismo independiente de control de SRF debe publicar informes anuales.
18. Se deben poner a disposición del organismo de control todas las evaluaciones de impacto antes del despliegue de cualquier sistema.

## Uso de SRF

**PRINCIPIO 1:** Las fuerzas de seguridad no deben usar SRF o recolectar, guardar, usar o divulgar información personal relacionada con el uso de SRF a menos que dichas acciones estén autorizadas por una ley específica.

La ley debe detallar las circunstancias estrictas bajo las cuales se autoriza el uso de SRF y debe estar escrita de forma que garantice que la ciudadanía y residentes puedan comprender y prever las condiciones y circunstancias precisas en las cuales se utilizan o utilizarán SRF.

Esta ley también debe establecer de forma expresa que los SRF nunca deben usarse para:

- Identificar a alertadores (*whistleblowers*), periodistas o fuentes periodísticas;
- Identificar a personas sobre las que no exista evidencia, directa o indirecta, de su relación con un crimen;
- Clasificar a las personas por su pertenencia a grupos protegidos o en relación con un sistema de puntaje social (*social scoring*);
- Intentar inferir las emociones o intenciones de una persona;
- Intentar predecir las acciones futuras de una persona;
- Identificar a manifestantes o recolectar información de personas que asisten a protestas o manifestaciones; o
- Identificar a personas en centros de votación o sus alrededores.

Cualquier uso de SRF debe, como mínimo, respetar este y los siguientes principios:

## **BASE JURÍDICA**

**PRINCIPIO 2:** Toda base jurídica para el uso de SRF por una institución de las fuerzas de seguridad debe incluir la obligación indelegable de dicha entidad de realizar una serie de evaluaciones de impacto antes de cualquier nuevo despliegue. Estas evaluaciones deben incluir, pero no limitarse a, un examen de impacto sobre derechos fundamentales y un examen de estricta necesidad y proporcionalidad del uso del sistema.

La primera de estas debe identificar, evaluar y abordar los efectos adversos del uso del sistema sobre los derechos humanos. Este análisis debe presentar de forma explícita:

- los parámetros específicos de su uso, incluyendo quién lo utilizará, sobre quién, dónde, por qué, cómo y si es un sistema de tipo retrospectivo o iniciado por un operador;
- los derechos impactados, en particular el derecho a la privacidad, protección de datos personales, libertad de expresión y reunión pacífica y el derecho a la no discriminación;
- la naturaleza y alcance de los riesgos sobre esos derechos;
- cómo cada uno de esos riesgos será mitigado;
- una justificación comprobable de cómo y por qué los beneficios de uso superan los impactos sobre los derechos; y
- los recursos disponibles para la persona que haya sido identificada erróneamente<sup>1</sup> o cuyos datos biométricos hayan sido procesados cuando no deberían haberlo sido.

Todo análisis de estricta necesidad y proporcionalidad del uso de SRF debe detallar la necesidad de su uso para un objetivo preestablecido y legítimo e incluir:

- evidencia del problema que sería abordado por el uso de SRF;

---

<sup>1</sup> Para el propósito de estos principios, se entiende por “identificación errónea” o “errada” la elección incorrecta de una persona que un revisor humano realiza entre una lista de posibles candidatos de una búsqueda de sistema de reconocimiento facial. Hablamos de identificación errónea cuando a esta elección incorrecta le siguen acciones de las fuerzas de seguridad contra dicha persona, como ser incluida en una lista de sospechosos, ser interrogada, arrestada, detenida o procesada.

- una explicación basada en evidencias sobre por qué utilizar SRF sería realmente efectivo para abordar dicho problema; y
- evidencia de por qué otras medidas ya existentes y menos intrusivas que no involucran SRF no serían suficientes para alcanzar el objetivo legítimo.

Ninguna entidad podrá utilizar un sistema de reconocimiento facial para un uso distinto del original si una evaluación de impacto señala que dicho uso del sistema y la composición demográfica de los datos de entrenamiento pueden producir sesgos contra personas pertenecientes a grupos protegidos por su género, edad o pertenencia a un grupo étnico-racial, entre otras.

Ninguna institución de las fuerzas de seguridad podrá realizar un sistema de reconocimiento facial para un uso distinto del original si no es estrictamente necesario o proporcional.

Estas evaluaciones se realizarán todos los años para cada SRF tras su despliegue. Si un SRF en uso falla en cualquier evaluación de esta naturaleza, el sistema será retirado.

## **NO EXCLUSIÓN DE LA BASE JURÍDICA**

**PRINCIPIO 3:** Las obligaciones del Principio 2 se cumplirán con independencia de los posibles requisitos o requerimientos legales de los proveedores de SRF en relación con la publicación o divulgación de información sobre sus algoritmos y datos de origen.

## **EVALUACIÓN DE RIESGO DE DEPENDENCIA DE PROVEEDORES**

**PRINCIPIO 4:** Las fuerzas de seguridad no deben adquirir o desplegar ningún SRF nuevo sin una evaluación previa del riesgo de dependencia de proveedores (*vendor lock-in*), incluyendo, pero sin limitarse a:

- una evaluación de la interoperabilidad y compatibilidad con sistemas existentes;
- una evaluación de la propiedad y portabilidad de los datos que evalúe los costos de migrar datos a sistemas de proveedores diferentes;
- una comparación de los sistemas, componentes y algoritmos de propiedad con las alternativas abiertas existentes, si los hubiese; y
- una estrategia para cambiar proveedores si fuera necesario, incluyendo los costos previsibles de tal cambio.

La contratación y compra de SRF debe favorecer las ofertas de proveedores que maximicen los estándares abiertos e interoperabilidad y que minimicen los componentes propietarios.

Es obligación de los proveedores explicar, en lenguaje simple, cómo funciona un sistema específico de reconocimiento facial, y la obligación de las autoridades de las fuerzas de seguridad entender bien cómo funcionan la tecnología y el sistema.

Esta evaluación se realizará todos los años para cada SRF utilizado. Si aumentase el riesgo de dependencia de proveedores, se tomarán acciones para reducir la dependencia de terceros, incluyendo, de ser necesario, la remoción del SRF.

## **PUBLICACIÓN DE LOS RESULTADOS DE LA EVALUACIÓN DE RIESGO**

**PRINCIPIO 5:** Todas las versiones de todas las evaluaciones, incluyendo análisis de estricta necesidad y proporcionalidad y estudios de impacto en derechos humanos,<sup>2</sup> realizados antes de cualquier despliegue de SRF, y sus resultados, se deben hacer públicos antes de dicho despliegue de manera que maximice el alcance público, en especial entre las personas que tienen más posibilidades de ser objeto de usos específicos del SRF.

## **CONSULTA PÚBLICA**

**PRINCIPIO 6:** Antes del despliegue de un SRF por cualquier institución de las fuerzas de seguridad, esta debe realizar consultas públicas significativas, incluyendo a miembros de las comunidades que serán afectadas de forma desproporcionada por el uso del SRF. Estas consultas deben incluir:

- detalles de cómo funcionan la tecnología y el sistema concreto de manera clara y accesible;
- detalles de los parámetros del uso esperado por las autoridades dentro de la jurisdicción en cuestión, incluyendo las condiciones estrictas bajo las cuales el sistema será utilizado;
- detalles de las imágenes usadas como imágenes de consulta (*probe image*) y los dispositivo a través de los cuáles son capturadas;
- detalles de las imágenes que se incluyen en todas las bases de datos de referencia;

---

<sup>2</sup> Estas evaluaciones deben llevarse a cabo de acuerdo con las definiciones y estándares internacionales.

- datos demográficos sobre las personas que se espera sean objeto del uso del sistema;
- todas las evaluaciones requeridas bajo estos principios por escrito; y
- detalles de las garantías existentes para prevenir el uso arbitrario del sistema.

La consulta pública significativa también requiere lo siguiente:

- la publicación de todas las aportaciones hechas por miembros del público, personas expertas, sociedad civil u otros actores durante el proceso de consulta;
- el tiempo suficiente para que las autoridades reflexionen sobre dichas aportaciones antes de que se tome cualquier decisión con respecto al despliegue; y
- poner en marcha mecanismos y garantías para asegurar que el proceso de consulta influya, moldee e incluso cancele el despliegue.

## **IMAGEN DE CONSULTA**

**PRINCIPIO 7:** Las fuerzas de seguridad deben usar todas las herramientas disponibles para hacer públicos los detalles de cómo se usan las imágenes de consulta en el uso de SRF de forma clara e inteligible, en línea y fuera de línea, de forma que sea accesible para todas las personas. Estos detalles deben incluir, sin limitarse a:

- los criterios necesarios para que la imagen de una persona se convierta en una imagen de consulta;
- las fuentes de las imágenes de consulta;
- el tiempo que esas imágenes de consulta se retienen antes de ser destruidas;
- la base jurídica para la obtención, retención y procesamiento de imágenes de consulta; y
- los detalles de contacto del organismo de supervisión (ver el Principio 16) designado para garantizar los derechos fundamentales de las personas cuyas imágenes se usan en una búsqueda de SRF.

## **DIVULGACIÓN DE ESPECIFICACIONES Y POLÍTICAS TÉCNICAS**

**PRINCIPIO 8:** Antes de cualquier despliegue de SRF por una institución de las fuerzas de seguridad, esta debe divulgar los detalles de las especificaciones técnicas de cualquier SRF que planea usar de forma clara e inteligible. Estos detalles deben incluir, sin limitarse a:

- una descripción detallada de todos los componentes de hardware y software (incluyendo el nombre y fabricante, número de versión y año de desarrollo del algoritmo) que se usan en el sistema. Esto incluye servidores, bases de datos, equipo de red, cámaras y cualquier software o servicios de terceros integrados al sistema;
- un desglose del sistema en sus varios subsistemas y módulos con las descripciones de la funcionalidad y propósito de cada parte incluyendo tanto el algoritmo central de reconocimiento facial como cualquier sistema auxiliar como el preprocesamiento de imágenes, encriptación de datos y las interfaces de usuario;
- una representación visual del diseño y arquitectura del sistema que ilustre cómo se recopila, procesa, almacena y accede a la información. La misma debe incluir los puntos de entrada de datos, etapas de procesamiento, ubicaciones de almacenamiento de datos y procesos de recuperación de información;
- las tasas de error del SRF utilizado, incluyendo las tasas de falsos positivos y falsos negativos, así como la documentación sobre cómo se calculan dichas tasas de error, aclarando si reflejan pruebas (laboratorio) o condiciones operativas que reflejan la composición demográfica del lugar donde se empleará el sistema de reconocimiento facial; y
- una lista de parámetros usados por la base de datos de referencia que incluya:
  1. la base jurídica y los procedimientos internos a seguir antes de agregar a una persona a la base de datos;
  2. las fuentes de las imágenes contenidas en la base de datos;
  3. cuántas imágenes hay en la base de datos;
  4. cómo se obtuvieron esas imágenes;
  5. por cuánto tiempo se mantienen en la base de datos las imágenes almacenadas;

6. con cuánta frecuencia se limpia la base de datos;
7. el proceso para eliminar imágenes de la base de datos;
8. quién tiene acceso a la base de datos y cuándo / bajo qué circunstancias;
9. cómo se mantiene la base de datos;
10. la identidad de la persona/unidad responsable del mantenimiento y supervisión de la base de datos;
11. las políticas de privacidad y protección de datos aplicables a la base de datos de referencia;
12. cómo se evalúa y prueba, por parte de las instituciones de las fuerzas de seguridad, que la creación de una base de datos de referencia o la inclusión de una persona en dicha base cumple con los requisitos de necesidad y proporcionalidad; y
13. los criterios para la inclusión de una persona en la base de datos de referencia.

## **USOS PROHIBIDOS**

**PRINCIPIO 9:** Ningún SRF será usado en imágenes en movimiento o datos de video en vivo o grabados.<sup>3</sup>

## **AUTORIZACIÓN JUDICIAL PREVIA**

**PRINCIPIO 10:** Los integrantes de las fuerzas de seguridad no podrán usar SRF a menos que haya una autorización judicial previa para dicho uso, excepto en casos urgentes debidamente justificados con la aprobación de un superior completamente independiente de la investigación. En esos casos excepcionales, la autorización judicial deberá solicitarse sin retrasos injustificados y no más tarde de 48 horas tras el uso del sistema.

---

3 Como ejemplo de situaciones cubiertas por este principio, ver Escenario 3, página 47 de las [Directrices 05/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley del CEPD](#) y la sección 307.5 - 3.2 del [manual sobre el uso de SRF del departamento de la policía de Detroit \(DPD\)](#) de 2024, que prohíbe el uso de SRF en transmisiones en vivo o videos grabados. Establece que: “Los miembros (del departamento de policía) no usarán Reconocimiento Facial en transmisiones en vivo o videos grabados. Esta prohibición se aplica a todos los videos, ya sean producidos por el mismo DPD, ciudadanos o ciudadanas particulares o cualquier otra fuente”.

Cualquier oficial de las fuerzas de seguridad realizando una búsqueda retrospectiva con SRF debe ser independiente de la investigación del ilícito, y cualquier oficial de las fuerzas de seguridad que use SRF debe haber completado un entrenamiento de uso, que será actualizado todos los años.

Este entrenamiento se enfocará en cómo usar el sistema en cuestión, cómo evaluar los impactos que el uso del sistema tiene sobre los derechos humanos, cómo determinar si el uso es estrictamente necesario y proporcionado y cómo cumplir de modo integral las previsiones de la ley que regula el uso de SRF.

## **REGISTRO DE USO**

**PRINCIPIO 11:** Las fuerzas de seguridad deben documentar cada búsqueda realizada en un sistema de reconocimiento facial, retrospectivo o iniciado por operador, y presentar esta documentación al organismo de control cada trimestre. Esta documentación incluirá lo siguiente:

- **en relación con el uso de sistemas retrospectivos**, una copia de la solicitud escrita de búsqueda en el sistema, que debe incluir:
  - la fecha y hora de la solicitud;
  - el nombre y posición del oficial solicitante e institución de las fuerzas de seguridad a la cual pertenece;
  - detalle de la necesidad y proporcionalidad de la solicitud;
  - la motivación de la solicitud, incluyendo, pero no limitándose a, cualquier crimen subyacente sospechado;
  - el nombre de la autoridad judicial ante la cual se realizó la solicitud y, en caso de circunstancias excepcionalmente urgentes, el nombre del oficial de mayor rango que dio la autorización temporal;
  - el resultado de la solicitud; y
  - si la solicitud fue aprobada, la composición de la base de datos de referencia utilizada en la búsqueda.
- en el caso de **uso de sistemas tanto retrospectivos como iniciados por operador**, la documentación debe incluir:
  - el resultado de cada búsqueda, el número de posibles coincidencias obtenido en cada una y todas las acciones tomadas por las fuerzas de seguridad subsecuentes a cada búsqueda.

- el nombre y posición del oficial que llevó a cabo la búsqueda; e
- información agregada sobre el uso del sistema, incluyendo:
  - el número total de solicitudes de búsqueda en el sistema;
  - el número total de solicitudes de búsqueda que generaron pistas;
  - el número de búsquedas que derivaron en arrestos o cargos;
  - el número de identificaciones erróneas;<sup>4</sup>
  - el número de personas que figuran como una posible correspondencia en la búsqueda y que fueron cuestionadas, arrestadas o acusadas como consecuencia;
  - un desglose demográfico de las personas en imágenes de consulta por género y pertenencia a un grupo étnico-racial; e
  - información sobre el sistema y algoritmo(s) usado(s), incluyendo los proveedores, la versión, el umbral de identificación y si se ajustó dicho umbral para esta búsqueda específica.

Además de lo anterior, toda base de datos de imágenes usadas por las fuerzas de seguridad para una búsqueda con SRF debe ser auditada al menos una vez al año para asegurarse de que no contenga imágenes que ya no deban ser retenidas, que no contenga información incorrecta y que no sea accedida o usada de forma inapropiada o ilegal. Estas auditorías también deben presentarse al organismo de control.

Cualquier otra información requerida por el organismo de control para cumplir con sus obligaciones debe ser presentada en tiempo razonable.

## **PROHIBICIÓN DE ACCIÓN**

**PRINCIPIO 12:** Un oficial de las fuerzas de seguridad no cuestionará, arrestará, detendrá o tomará ninguna acción contra una persona basándose únicamente en el uso de SRF. El uso de SRF no resultará en la inclusión de alguien en una ronda de reconocimiento fotográfica o física. Los oficiales de las fuerzas de seguridad también tienen prohibido actuar solo sobre la base de la combinación de una pista resultante de un SRF y la confirmación de identidad provista por un testigo o por otro proceso de confirmación de identidad, como una ronda de reconocimiento

---

4 Como está definido en la nota al pie del Principio 2

fotográfica o física. El resultado de un sistema de reconocimiento facial es solo una pista a investigar. No representa una prueba confiable y cualquier resultado de un SRF debe seguirse de acciones investigativas independientes y fiables antes de que un oficial de las fuerzas de seguridad tome acción alguna.

## **OBLIGACIÓN DE DIVULGAR**

**PRINCIPIO 13:** Las fuerzas de seguridad deben informar a las personas detenidas, cuestionadas, arrestadas, acusadas o procesadas como consecuencia del uso de SRF y a su representante legal (si corresponde), sin restricciones, los detalles y las especificaciones técnicas del sistema usado en la investigación o procedimiento. Estos detalles deben incluir todo lo especificado en el Principio 8 y además:

- el código fuente para cada algoritmo utilizado;
- los datos usados para el entrenamiento y afinación (*fine-tuning*) del sistema;
- una lista de métricas, puntos nodales u otras marcas únicas de identificación usadas por el sistema al crear los vectores de rasgos faciales, incluyendo los pesos que recibe cada marca, en su caso;
- acceso a un entorno de prueba con una versión ejecutable del software;
- la copia original de la imagen de consulta que se usó;
- cualquiera y toda información asociada a la imagen de consulta, incluyendo los metadatos que estaban en posesión, o se pusieron a disposición, de la persona que realizó la búsqueda con el sistema;
- detalles del umbral de identificación del sistema fijado por el fabricante (y por las fuerzas de seguridad si cambian dicho umbral) para determinar cuando el programa en cuestión indica que hay una posible coincidencia; y
- en el caso particular de uso de un sistema retrospectivo:
  - todas y cada una de las copias de la imagen de consulta usada especificando, en su caso, qué copia editada dio como resultado la lista de candidatos donde estaba la persona acusada, junto con una lista de ediciones, filtros o cualquier otra modificación hecha a dicha imagen;
  - una copia de la imagen de la base de datos que emparejada con la imagen de consulta y el número de posición y puntajes de similitud asignados a la imagen por el sistema de reconocimiento facial en la lista de posibles coincidencias;

- una lista o descripción del número de posición o puntajes de similitud producidos por el sistema de reconocimiento facial que incluya la escala sobre la que el sistema se basa;
- una copia de la lista completa de posibles coincidencias producida por el sistema de reconocimiento facial en orden de posición y con el puntaje de similitud asignado a cada imagen por el sistema;
- el informe escrito producido por la persona que realizó la búsqueda en el sistema de reconocimiento facial, incluyendo la fecha, hora de la búsqueda y cualquier nota sobre la posible coincidencia con cualquier otra persona de la lista de candidatos; y
- el nombre y capacitaciones, certificaciones o calificaciones de la persona que realizó la búsqueda con el sistema de reconocimiento facial.

## **INFORME DE IDENTIFICACIONES ERRADAS**

**PRINCIPIO 14:** Cualquier identificación errónea de una persona debe reportarse a esta por la entidad de las fuerzas de seguridad lo antes posible después de que dicha identificación errónea haya sido descubierta y registrada.

## **INFORME ANUAL DE IDENTIFICACIONES ERRADAS**

**PRINCIPIO 15:** Las fuerzas de seguridad que usan SRF deben producir un informe anual con las estadísticas anonimizadas sobre identificaciones erróneas. Estos informes deben incluir la naturaleza, fuente e impacto del error y las medidas tomadas por las autoridades en respuesta a las identificaciones erróneas, quiénes operaron el sistema y los procedimientos y protocolos aplicables a dicho uso. Estos informes deben ser de acceso público y presentados al organismo de control previsto en el Principio 16.

## **ORGANISMO INDEPENDIENTE DE CONTROL**

**PRINCIPIO 16:** Se establecerá un organismo independiente de control antes de cualquier despliegue de SRF por parte de las fuerzas de seguridad para evaluar el uso de estos sistemas y su adecuación, o no, a la regulación de derechos fundamentales, demás regulación aplicable y estos principios. Este organismo debe:

- estar establecido y regulado por ley;

- estar separado, y ser independiente, del ejecutivo nacional o estatal (o equivalente);
- tener los fondos, capacidades, experiencia y personal, tanto legales como tecnológicos, necesarios para cumplir con sus funciones;
- contar con acceso libre e inmediato a la información necesaria que requiere para cumplir con sus funciones;
- informar todos los años al público sobre su trabajo y conclusiones; e
- informar todos los años al parlamento.

El organismo de control será provisto de las capacidades y recursos necesarios para desarrollar una metodología de evaluación para el análisis de uso de SRF y su adecuación, o no, a la regulación de derechos fundamentales, demás regulación aplicable y estos principios. La metodología de evaluación debe incluir el conjunto de requisitos mínimos que un sistema de reconocimiento facial debe cumplir; por debajo de los cuales, el sistema debe ser retirado.

El organismo de supervisión tendrá el poder de ordenar el retiro de un sistema de reconocimiento facial cuando este no cumpla con dichos requisitos mínimos.

## **INFORME ANUAL DEL ORGANISMO INDEPENDIENTE DE CONTROL**

**PRINCIPIO 17:** El organismo independiente de control de SRF descrito en el Principio 16 publicará informes anuales que contendrán todas las evaluaciones escritas mencionadas en estos principios y además:

- una evaluación detallada y comentario de la base jurídica aducida por las fuerzas de seguridad para el uso de SRF;
- el número de imágenes de consulta individuales usadas en búsquedas con SRF;
- el número de imágenes usadas como referencia y en bases de datos;
- el número de coincidencias correctas y falsos positivos por cada uno de los despliegues;
- el número de arrestos por cada uno de los despliegues;
- el número de detenciones y registros por cada uno de los despliegues;
- el número total de solicitudes de uso de SRF realizadas;
- el número total de despliegues de SRF;

- el número de solicitudes o búsquedas hechas con autorización judicial;
- el número de solicitudes o usos de emergencia realizados; y
- las razones de la solicitud de búsqueda, incluyendo, pero no limitándose a, cualquier crimen subyacente sospechado.

## **NOTIFICACIÓN PREVIA DE LAS EVALUACIONES DE IMPACTO AL ORGANISMO DE CONTROL**

**PRINCIPIO 18:** Además del Principio 5, los detalles y conclusiones de cada evaluación de impacto, como están descritas en los Principios 2 y 3, deben ponerse a disposición del organismo de control antes de que se despliegue el sistema de modo que se puedan analizar y evaluar dichas conclusiones de las fuerzas de seguridad.

## **Palabras finales**

Quienes escribieron y contribuyeron a este informe opinan que los sistemas de reconocimiento facial no deben ser usados por la policía y fuerzas de seguridad. Como se explica de forma exhaustiva a lo largo de todo este informe, los riesgos y posibles perjuicios asociados al uso de estos sistemas son mayores que cualquier posible beneficio. Los daños significativos, tanto a la privacidad como a la confianza de la sociedad en sus instituciones, hacen que su uso en un contexto policial sea injustificable.

# Agradecimientos

Este proyecto fue desarrollado, redactado y editado por Olga Cronin (INCLO/ICCL), Víctor Práxedes Saavedra Rionda (INCLO), Elizabeth Farries (Centro de Políticas Digitales de University College Dublin), Kirill Koroteev (Agora) y Timilehin Ojo (INCLO/CCLA).

Los principios fueron elaborados tras la reunión anual de INCLO en 2023. Fue ahí que se identificó la falta generalizada de conocimientos técnicos y jurídicos sobre el uso del reconocimiento facial por las fuerzas de seguridad y la preocupación que generaba esa falta en los países miembros. A lo largo de 2023 y 2024, especialistas en derechos humanos provenientes de los campos del derecho, la tecnología, la sociología y la comunicación se reunieron para desarrollar esta lista de principios.

Este es un esfuerzo colaborativo de las 15 organizaciones miembros de INCLO en este entonces. Por sus aportes al desarrollo, estudio de caso, redacción, edición e investigación, INCLO agradece sinceramente a: Lucila Santos, Myriam Selhi (INCLO), Vanessa Lopez (Dejusticia), Sherylle Dass (LRC), Devon Turner (LRC), Manuel Tufro (CELS), Ben Wizner (ACLU), Kieran Pender (HRLC), David Mejía-Canales (HRLC), Martin Mavunjina (KHRC), Gil Gan-Mor (ACRI), Anaïs Bussièrès McNicoll (CCLA), Karim Medhat Ennarah (EIPR), Sehba Meenai (HRLN), Rempport Ádám (TASZ), Nadine Sherani (KontraS), Emmanuelle Andrews (Liberty), Nathan Freed Wessler (ACLU), Jun Pang (Liberty), Daniel Konikoff (CCLA) y Daniel Ospina Celis (Dejusticia).

INCLO agradece a Taryn McKay por el diseño, a Sam Kelly por la edición en inglés, a Malena Saralegui por la traducción al español y a Alina Najlis por las ilustraciones.

Lee el informe completo en [inclo.net/frt](https://inclo.net/frt)