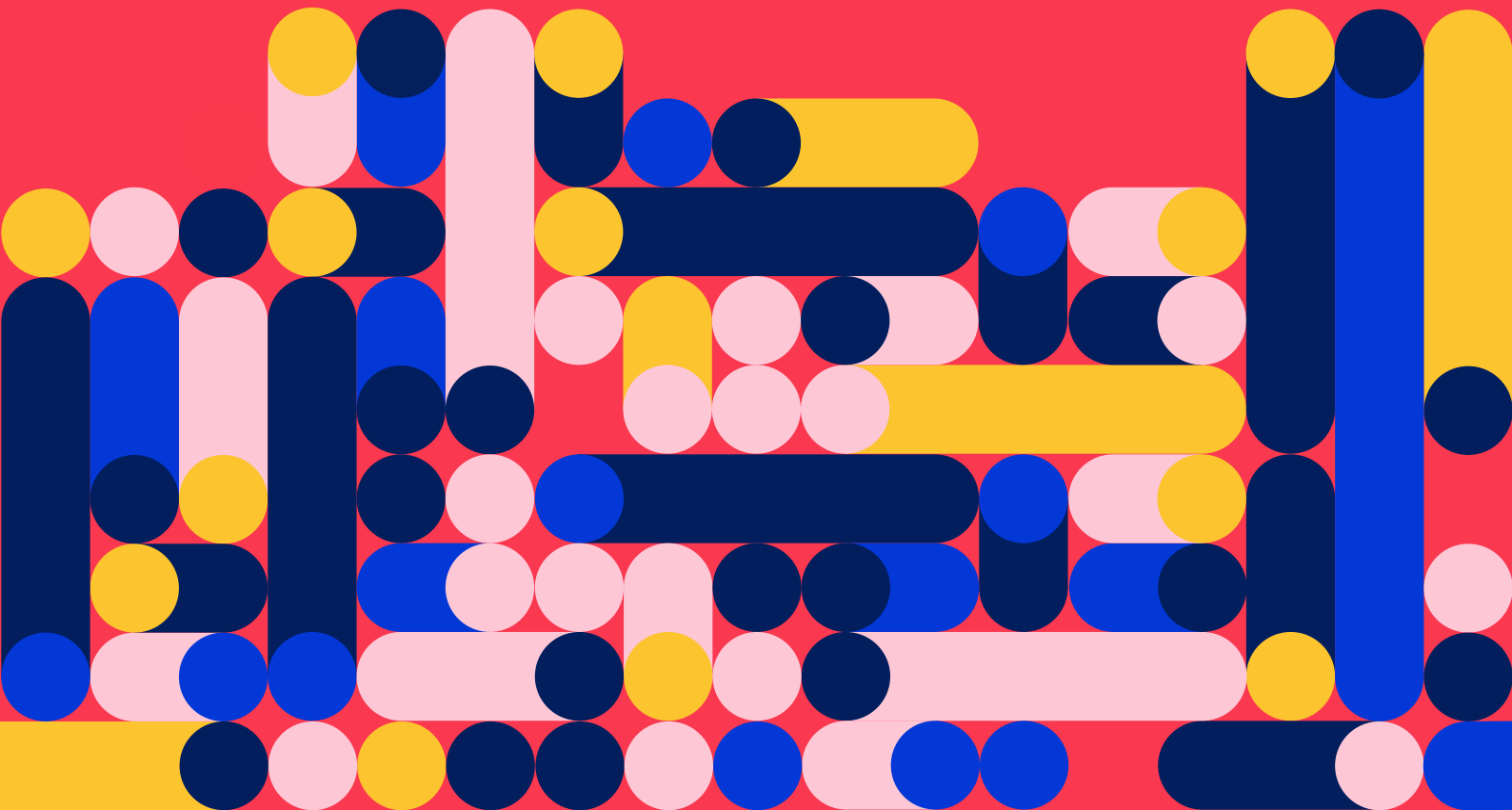
Reconocimiento facial en América Latina

Tendencias en la implementación de una tecnología perversa

AlSur



Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa

Texto: Jamila Venturini y Vladimir Garay (Derechos Digitales)
Revisión: María Paz Canales (Derechos Digitales), Juan Diego Castañeda (Fundación Karisma) y Cristin León (Al Sur).
Traducción al portugués: Dafne Melo.
Traducción al inglés: Pedro Nogueira.
Diagramación: Rocío Rubio.
Gráficos: Data Sketch.

Recolección de datos: Abdías Zambrano (Ipandetec), Alejo Kiguel (ADC), Bárbara Simão (Internet Lab), Dilmar Villena (Hiperderecho), Joana Varon y Vanessa Koetz (Coding Rights), Juliana Valdés, Juan Diego Castañeda y Joan López (Fundación Karisma), Luã Cruz (IDEC), Maricarmen Sequera (TEDIC), Michele Bordachar (Derechos Digitales), Santiago Narváez (R3D).

Con el apoyo de

AlSur

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

A modo de introducción

El reconocimiento facial es una tecnología de identificación biométrica que, por medio del análisis de ciertos rasgos característicos del rostro, busca establecer la identidad de una persona. A pesar de ser menos precisa que otras formas de identificación biométrica, como la lectura de huellas dactilares o del iris, no requiere contacto físico. Ello permite su despliegue, por ejemplo, en el espacio público con fines de vigilancia a gran escala y sin que quienes están siendo sujetos a su escrutinio sean necesariamente conscientes de ello.

Aunque su introducción se remonta a la década del 60, distintos avances técnicos recientes han sido claves para su aplicación en los últimos años. El desarrollo de nuevas tecnologías para la captura y procesamiento de imágenes, los avances en el campo del "big data" —asociados a la recolección, almacenamiento y tratamiento de grandes volúmenes de datos— así como también los avances en las técnicas de "aprendizaje profundo" (*Deep Learning*) en el "entrenamiento" de algoritmos, han facilitado la adopción cada vez mayor de los sistemas de reconocimiento facial en distintos ámbitos. Hoy, el reconocimiento facial tiene aplicaciones variadas que van desde el desbloqueo de dispositivos móviles hasta los intentos por "leer" intencionalidades y emociones, uso que le emparenta con las técnicas y teorías frenológicas desarrolladas en el siglo XIX.

Si bien los sistemas de reconocimiento facial pueden ser diversos, todos requieren de al menos tres elementos para funcionar: una forma de capturar imágenes, un software encargado del análisis de las imágenes y una base de datos con rostros para hacer la comparación. La precisión del sistema dependerá del acceso a una base de datos que permita la identificación de las imágenes con sujetos previamente catalogados, de que las imágenes cumplan con ciertos estándares mínimos de calidad requeridos por el software para su análisis (tamaño, luminosidad, que la imagen capture los puntos de análisis utilizados por el sistema, etc.), del modo en que los algoritmos hayan sido "entrenados" para hacer las asociaciones entre los datos capturados y aquellos en la base de datos que permite la comparación, así como del diseño mismo del software, que indicará los parámetros precisos de acuerdo a los que se efectuarán las comparaciones para producir la identificación. Problemas en cualquiera de estos niveles pueden impedir que el sistema realice correctamente la función para la cual ha sido implementado, lo que puede traducirse en reconocimientos fallidos, discriminaciones arbitrarias y falsos positivos, todas situaciones —lamentablemente— comunes asociadas al uso de sistemas de reconocimiento facial, especialmente cuando se utiliza para vigilar el espacio público y para resguardar el acceso a derechos sociales.

Este problema se incrementa dramáticamente cuando las personas sujetas a esta tecnología pertenecen a grupos históricamente vulnerados como mujeres, personas de piel oscura o personas trans. Así, la implementación de sistemas de reconocimiento facial conlleva la reproducción técnica de los sesgos de exclusión social y, cuando son utilizados con fines de vigilancia, amenazan el derecho a la dignidad, al debido proceso y la presunción de inocencia, entre otros.

Por tratarse de una tecnología de identificación biométrica, es decir, que procesa información relativa a nuestros cuerpos, el reconocimiento facial es una técnica altamente intrusiva y que fuerza la recolección y almacenamiento de un dato sumamente íntimo, quitándonos control sobre nuestro rostro y avalando su uso potencialmente contra nuestros propios intereses y beneficios.

Cuando se utiliza para la vigilancia del espacio público y el combate del delito común, el reconocimiento facial erosiona la autonomía de las personas en favor de un sistema que pretende el control absoluto, mediante la gestión técnica de las identidades, reproduciendo las desigualdades y exclusiones que históricamente han puesto en desventaja a las comunidades no hegemónicas.

El objetivo de esta investigación es incentivar el debate público respecto al modo en que los sistemas de reconocimiento facial han avanzado en América Latina, a partir de la iniciativa estatal. Tales desarrollos han estado marcados por una opacidad excesiva y por escasos compromisos por parte de las autoridades que garanticen condiciones mínimas en su despliegue, para mitigar impactos en el ejercicio de derechos fundamentales.

¿Cuáles son las tecnologías de reconocimiento facial presentes en la región? ¿Para qué se usan? ¿Quién las provee? ¿Cómo están reguladas? ¿Cómo son auditadas? Estas son algunas de las preguntas que esta investigación intenta responder.

El informe se inicia con la explicación de la metodología utilizada para la recopilación de información sobre las iniciativas seguido de un panorama de las tendencias observadas en la región y un análisis más detenido de las empresas proveedoras de tecnologías de reconocimiento facial. Finalizamos con algunas consideraciones sobre los impactos observados de las iniciativas identificadas.

Mapeando el reconocimiento facial en América Latina

El presente informe presenta un análisis cualitativo en base a los hallazgos del levantamiento de información sobre el despliegue de sistemas de reconocimiento facial en nueve países de América Latina, llevado a cabo entre abril y mayo de 2021. La investigación fue desarrollada por las organizaciones que forman parte del Consorcio AI Sur, a partir de una metodología propuesta por las siguientes organizaciones: Coding Rights, IPANDETEC, InternetLab, R3D, Derechos Digitales, TEDIC y Fundación Karisma.

El objetivo de la investigación fue mapear detalladamente las iniciativas existentes en la región, con especial énfasis en identificar las empresas proveedoras de tecnologías biométricas dominantes y sus países de procedencia, el tipo de relación establecida con los Estados, las áreas en que predomina su presencia y sus potenciales consecuencias sociales, económicas y políticas. Por ese motivo, el análisis se centra en las iniciativas desplegadas por iniciativa del Estado, aunque se reconoce la existencia de una serie de aplicaciones de sistemas de reconocimiento facial impulsada por el sector privado con gran potencial de afectación a derechos fundamentales. Además, la presente investigación está considerada como el primer paso de un esfuerzo más amplio de mapeo de tecnologías de identificación biométrica en América Latina.

Este informe está complementado por el sitio web https://estudio. reconocimientofacial.info/, donde es posible encontrar más detalles sobre cada una de las iniciativas encontradas, las proveedores de tecnologías y más información sobre las tendencias regionales en la implementación de sistemas de reconocimiento facial en la región. Además, en reconocimientofacial.info es posible encontrar noticias y novedades sobre acciones de resistencia a la implementación de estos sistemas, modelos de solicitud de acceso a la información, entre otras informaciones.

Metodología

El ejercicio de identificación y caracterización de los sistemas de reconocimiento facial presentes en la región y las entidades encargadas de proveer e implementar dicha tecnología se realizó mediante la confección de fichas estandarizadas, que dan cuenta de información relevante, incluyendo área de aplicación, estado actual de funcionamiento de la iniciativa, país de procedencia de los proveedores y sector al que pertenecen, características del contrato, existencia de estudios de impacto previos y auditorías posteriores a la implementación del sistema, entre otros. El objetivo fue poder tipificar la información, de modo que sea comparable para facilitar la identificación de tendencias regionales.

Se consideraron sistemas de reconocimiento facial desarrollados en el marco de políticas públicas, especialmente aquellos sistemas implementados para asistir la vigilancia del espacio público y la autentificación de identidad, particularmente como medida de acceso a derechos y beneficios sociales. No se consideraron aquellos sistemas desplegados en espacios privados como tiendas, centros comerciales o bancos privados; tampoco están incluidos sistemas implementados en ámbitos como el comercio electrónico o el acceso a dispositivos digitales o aplicaciones cuando no constituyen un condicionante para el acceso a un servicio público.
La información recopilada en las fichas considera los siguientes aspectos:

- País
- Nombre de la iniciativa
- Descripción del sistema
- Área de aplicación
- Tipo de uso
- Fecha de implementación
- Estatus actual de la iniciativa
- Proveedores de tecnología involucrados
    - Nombre
    - País
    - Sector (gubernamental, privado, académico, sociedad civil)
    - Sitio web
    - Tipo de contrato (directo, licitación, donación)
    - Detalles de contratación

- ¿Hay alguna base legal o normativa que avale la implementación?
- ¿Hubo algún proceso de participación pública antes de la implementación?
- ¿El proceso de implementación consideró la realización de un estudio de impacto en privacidad y/o derechos humanos?
- ¿Está prevista alguna auditoría externa de la implementación?
- ¿Hay registros de incidentes de seguridad, usos discriminatorios u otros tipos de abusos relacionados con la iniciativa desde su implementación?
- Organización que llenó la ficha

La información fue compilada a partir de las siguientes fuentes:

- Solicitudes de acceso a la información.
- Entrevistas semiestructuradas con agentes clave: empresas, agentes públicos, etc.
- Búsqueda por palabras-clave en mecanismos de búsqueda: buscadores diversos en internet, medios de comunicación, portales de transparencia, webs de gobiernos, etc.
- Consulta a organizaciones de derechos humanos, movimientos sociales, periodistas y activistas en cada país.

¿Qué, cómo, dónde? Tendencias regionales sobre la implementación de reconocimiento facial en América Latina?

En el marco de esta investigación han sido mapeadas 38 iniciativas de uso de reconocimiento facial, repartidas en nueve países latinoamericanos e implementadas al alero de distintas políticas públicas. Si bien no se trata de un listado taxativo de la totalidad de sistemas existentes en la región, las cifras sirven para tener una idea general del panorama latinoamericano en torno al avance de esta tecnología y su desarrollo.

La mayor parte de los sistemas de reconocimiento facial documentados en la investigación datan de los últimos tres años, con tan solo siete de ellos implementados en una fecha previa a 2018. De los 38 sistemas listados, 22 se encuentran actualmente activos, cinco han sido desactivados, tres se encuentran en etapa piloto y ocho se encuentran en proceso de implementación.

Respecto a los cinco sistemas que han sido desactivados, en dos casos fue una orden judicial la que impidió la continuidad de su funcionamiento y uso, ambos en Brasil ("ViaQuatro"[1] y "Edital de Licitação do Metrô de São Paulo").[2] En otros dos casos los sistemas nunca se implementaron (el "Sistema Integrado de Videovigilancia Inteligente para Transmilenio en Colombia"[3] y la "Fórmula anti evasión Transantiago y Metro de Valparaíso" en Chile) y uno fue dado de baja por fallas, interrupciones y falta de medidas de seguridad ("Aplicación móvil de reconocimiento facial para entregar la Clave Única" en Chile).[4]

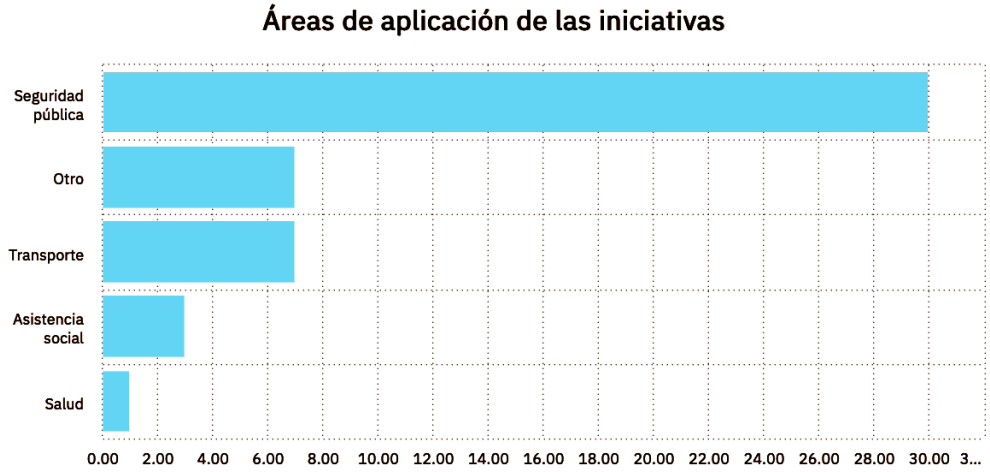
Respecto a las áreas de aplicación de los sistemas, por lejos el uso más recurrente es "seguridad pública" (30 sistemas listados) y "vigilancia de espacios públicos" (31 sistemas listados). Le siguen transporte (7 sistemas listados), asistencia social y migración (3 sistemas, respectivamente). En el marco de esta investigación no fue posible documentar sistemas de reconocimiento facial implementados en el campo de la educación ni en procesos electorales, pese a que se trata de ámbitos en que anecdóticamente —y sobretodo en el contexto de pandemia— se han visto incrementadas su implementaciones. Por su parte, se señala que 10 iniciativas se utilizan para el control de acceso a derechos económicos, sociales y culturales, tales como beneficios sociales otorgados por el Estado, mientras que el uso de seis de ellas dice relación con el control de acceso a derechos civiles y políticos, como acceso a la identificación por parte de la ciudadanía.

1 Ver https://reconocimientofacial.info/reconhecimento-facial-a-banalizacao-de-uma-tecnologia-controversa/

2 Ver https://reconocimientofacial.info/justicia-brasilena-condena-empresa-de-metro-por-uso-de-reconocimiento-facial-sin-consentimiento-en-sao-paulo/

3 Ver https://digitalid.karisma.org.co/2021/07/01/SIVIT-reconocimiento-facial/

4 Ver https://www.biobiochile.cl/noticias/nacional/chile/2020/03/29/registro-civil-anuncio-que-bajo-la-app-para-obtener-clave-unica-hubo-denuncia-sobre-su-seguridad.shtml



Respecto a las bases normativas que regulan la implementación de la tecnología de reconocimiento facial, es importante mencionar que en más del 60% de los casos no existe una base legal específica que avale la implementación. Solamente en 14 de los 38 casos documentados se señala la existencia de una normativa que sustentaría el despliegue de este tipo de tecnología. Sin embargo, llama la atención que en la mayor parte de los casos las normas citadas no son específicamente para la utilización de reconocimiento facial o datos biométricos, sino que se trata de una interpretación amplia de normativas referidas al uso de otro tipo de tecnologías (por ejemplo, el funcionamiento de cámaras de videovigilancia) que se quieren analogar al reconocimiento facial con argumentos dudosos o de facultades específicas que podrían cumplirse mediante la utilización de reconocimiento facial ("supervigilar el cumplimiento de disposiciones sobre evasión en el transporte público", "funciones de verificación migratoria, de extranjería y de control migratoria", etc.)

Pocos son los casos en los que se señala una normativa específica que aluda al reconocimiento facial u otras tecnologías de identificación biométrica. Ejemplos de ello serían la Portaria no 1.515 de 18 de diciembre de 2018 del Departamento Nacional de Tránsito – DENATRAN en Brasil, que habilitaría la implementación de la recolección y almacenamiento de datos biométricos para el otorgamiento de licencias de conducir,[5] la normativa que regula el Sistema Público Integral de Video Vigilancia creado por la ley de la Ciudad de Buenos Aires N. 5688 en Argentina[6] y el proyecto de ley 234 en Colombia,[7] que establece que la Registraduría Nacional del Estado Civil podrá identificar y autenticar nacionales en medios digitales en Colombia a través de "todo tipo de biometría" y que está siendo revisado por la Corte Constitucional. Incluso a nivel de protección de datos personales, en aquellos países en donde existen normas generales, las referencias a la regulación específica del uso de datos biométricos escasean. En opinión de los distintos expertos locales, ninguna de las normativas utilizadas para justificar la implementación de los sistemas de reconocimiento facial ofrece un tratamiento adecuado desde el punto de vista de los derechos humanos.

Este contexto normativo deficiente agrava los riesgos que este tipo de tecnologías presentan al ejercicio de derechos fundamentales. Es necesario además mencionar que la mayoría de los intentos por regular las tecnologías de identificación biométrica parecen estar más preocupados por validar su implementación que de balancear sus propósitos con el respeto de los derechos

5 Ver https://www.legisweb.com.br/legislacao/?id=372479

6 Ver http://www2.cedom.gob.ar/es/legislacion/normas/leyes/ley5688.html

7 Ver http://leyes.senado.gov.co/proyectos/index.php/textos-radicados-senado/p-ley-2020-2021/2021-proyecto-de-ley-234-de-2020

de la ciudadanía. En ese sentido, si bien es cierto que una regulación específica puede ser beneficiosa cuando busca subsanar deficiencias de la normativa general de protección de datos personales, eso solo será posible cuando su formulación considere un enfoque de prevención de riesgos de impacto en el ejercicio de derechos fundamentales, entre ellos notablemente privacidad y no discriminación.

En la gran mayoría de los casos, los sistemas de reconocimiento facial identificados en el marco de este estudio fueron implementados sin ningún tipo de consulta o participación pública, con la excepción de un sistema de vigilancia en Chile, iniciativa de cuya discusión participaron los Consejeros regionales, representantes elegidos popularmente y que forman parte de la estructura de gobierno regional descentralizado del país. En la discusión de la ley que rige el Sistema de Reconocimiento Facial de Prófugos en Buenos Aires, distintas organizaciones tuvieron posibilidad de presentar cartas manifestando sus preocupaciones,[8] pero no hubo una discusión en la Comisión de Derechos Humanos de la Legislatura de la Ciudad de Buenos Aires como estaba inicialmente previsto, lo que generó un importante reclamo por parte de la sociedad civil.[9] En el resto de las iniciativas no hubo ningún tipo de consulta abierta ni alguna instancia de participación pública respecto al diseño e implementación de los sistemas de reconocimiento facial.

Tampoco hubo estudios de impacto en privacidad o derechos humanos, entendidos los primeros como evaluaciones que miran a los riesgos de utilización de datos personales por un sistema para la autodeterminación informativa y la privacidad de sus titulares, mientras los segundos se pueden definir como un proceso para identificar, comprender, evaluar y abordar los efectos adversos de una actividad o política pública en el goce de los derechos humanos de los titulares de derechos afectados.

La única excepción es el Sistema de Reconocimiento Facial de Prófugos en Buenos Aires, que —en respuesta a una solicitud de acceso a la información pública realizada por la Asociación de Derechos Civiles— declara haber realizado "pruebas correspondientes a fin de reducir en la mayor medida admisible la tasa de error, junto con otras restricciones impuestas en torno a la conformación del registro de datos y las medidas de control del personal con acceso al sistema", y de esta manera minimizar los "impactos negativos en términos de derechos humanos".

En general, el desarrollo de auditorías externas al funcionamiento de los sistemas implementados tampoco es una práctica común. Las auditorías externas del funcionamiento de sistemas técnicos que impactan el ejercicio de derechos son una buena práctica que permite obtener información de forma independiente sobre el funcionamiento del sistema y los potenciales riesgos que su diseño o implementación puedan representar para el ejercicio de los derechos de los usuarios o personas impactadas por una tecnología específica. Su ausencia impide procesos iterativos de mejora en que la visión de los operadores del sistema sea complementada por visiones externas que contribuyan a su mejora y evitar impactos negativos de la implementación de un sistema.

Tan solo tres de las 40 iniciativas mapeadas dan cuenta de la realización de algún tipo de auditoría, dos en Colombia y una en Argentina. Respecto a los sistemas colombianos, hay un anuncio de la Alcaldesa Mayor de Bogotá sobre la eventual realización de auditorías externas a Ágata, Agencia de Analítica de Datos;[10] en el caso del Sistema Integrado de Videovigilancia Inteligente para Transmilenio —hoy desactivado— hubo una interventoría

8 Ver https://adc.org.ar/2020/09/18/avanza-la-regulacion-del-reconocimiento-facial-en-la-legislatura-portena

9 Ver https://www.telam.com.ar/notas/202010/527676-la-legislatura-aprobo-el-uso-de-reconocimiento-facial-para-la-detencion-de-profugos.html

10 Ver http://www.sdp.gov.co/noticias/agata-la-nueva-agencia-analitica-de-datos-hara-de-bogota-lider-global-transparencia-e-inteligencia

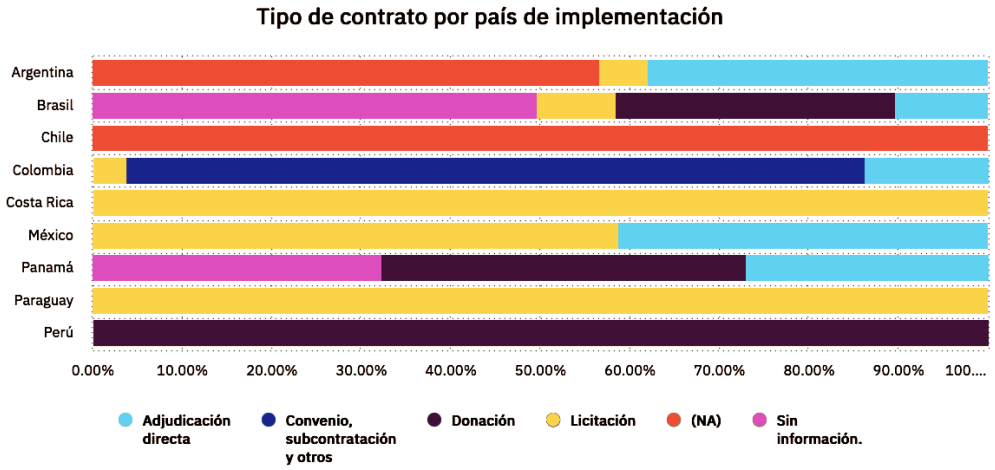
por la Universidad Francisco José de Caldas-IDEXUD a la instalación y funcionamiento de los equipos biométricos.[11]

Respecto al caso argentino, la ley que regula el funcionamiento del Sistema de Reconocimiento Facial de Prófugos en Buenos Aires considera la creación de una Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia, integrada por los/as Presidentes de las Comisiones de Justicia y de Seguridad, y tres diputados/as designados por la Vicepresidencia Primera del cuerpo, abriendo también la posibilidad de convocar a especialistas y organizaciones de la sociedad civil para analizar y proponer.[12]

Proveedores

Una diversidad de empresas está involucrada en proveer servicios para la implementación de iniciativas que utilizan tecnología de sistemas de reconocimiento facial en nuestra la región. Estas cumplen distintos roles, que van desde el despliegue de la infraestructura necesaria para la operación de esos sistemas, hasta la provisión de la tecnología de análisis biométrico. Si bien es relevante la participación de empresas locales, cabe observar que, por lo general, no son las responsables del desarrollo del software. En algunos casos, se especializan en la venta de sistemas desarrollados en el extranjero.

Es importante notar la presencia de empresas cuestionadas internacionalmente por su presunto involucramiento en la vulneración de derechos humanos. Es particularmente ilustrativo el caso de las empresas chinas Dahua y Hikvision, prohibidas de operar en Estados Unidos, mientras cuentan con contrataciones millonarias en México. La francesa IDEMIA (ex-Morpho Safran), presente en al menos cuatro países de la región, y la inglesa FaceWatch, cuyo software es utilizado en una de las iniciativas identificadas en Brasil, también han sido objeto de preocupaciones por parte de organizaciones internacionales.



Las empresas locales, a su vez, son muchas veces grandes proveedoras de servicios al Estado y, en varios casos, tienen alguna relación con figuras políticas o escándalos de corrupción.

11 Ver https://www.yumpu.com/es/document/read/55729155/informe20de20gestic3b3n202015

12 Ver http://www2.cedom.gov.ar/es/legislacion/normas/leyes/ley6339.html

Argentina

En Argentina se identificaron cuatro iniciativas de uso de sistemas de reconocimiento facial activas. Todas cuentan con la participación de empresas argentinas o multinacionales extranjeras, en algunos casos por medio de sus representantes locales.

- DANAIDE SA, contratada por 1.511.300 USD para ofrecer el servicio de análisis integral de video en el Sistema de Reconocimiento Facial de Prófugos (SRFP) implementado en la Ciudad Autónoma de Buenos Aires, activo desde 2019;
- NEC Argentina SA — parte del grupo global NEC CORPORATION de origen japonés —, contratada por 44.906.400 ARS (462.702 USD aproximadamente)[13] a partir de un proceso de licitación para ofrecer servicios de hardware, software y mantención en el Sistema de Reconocimiento Facial de Tigre NeoCenter, en la localidad de Tigre, provincia de Buenos Aires, activo también desde 2019;
- Nubicom, contratada para la implementación del sistema Reconocimiento Facial Salta en la ciudad de Salta, capital de la provincia, y activo desde 2018;
- Morpho Safran (actualmente IDEMIA), francesa, y DATYS, cubana, contratadas para pro veer la tecnología detrás del Sistema Federal SIBIOS de Identificación Biométrica para la Seguridad, activo desde 2011.

Además de las empresas identificadas, el software de reconocimiento facial utilizado en la SRFP y denominado UltraIP sería desarrollado por la empresa rusa NtechLab. Según fuentes periodísticas, el sistema sería utilizado en más de 3000 cámaras de videovigilancia en Rusia.[14]

La modalidad de contratación de las empresas, en los casos en que los datos estaban disponibles, fue de contratación directa en la Ciudad de Buenos Aires y de Salta. De acuerdo con la prensa local, la contratación de DANAIDE SA había sido denunciada por la actual vicepresidenta argentina Cristina Fernandez de Kirchner por espionaje en 2018.[15]

En el caso de Salta, la empresa inicialmente contratada para ofrecer los dispositivos de videovigilancia y el software al sistema Reconocimiento Facial Salta fue DATANDHOME SUPPLIER SA. Nubicom era la proveedora del servicio de conectividad. Sin embargo, el contrato con la primera fue rescindido en 2019 debido a "incumplimientos graves" en la instalación de las cámaras comprometidas. Por ello se suscribió una contratación directa con Nubicom, que quedó a cargo además de la conectividad y el mantenimiento de las cámaras y del software.

Según informaciones de la prensa, la contratación de Nubicom ha sido marcada por una serie de vicios, incluida un procedimiento abreviado por razones de emergencia que no fueron explicitadas. El costo mensual cobrado por la empresa para la provisión de servicios llegaría a los 440 mil dólares, según la misma fuente. Por su parte, DATANDHOME presentó una demanda judicial por 6 millones de dólares a la provincia de Salta por incumplimiento en los pagos.[16]

---

13 La conversión de los valores en moneda local a dólares estadunidenses implica una estimación para fines de referencia. Se hizo a partir de consulta a https://www.xe.com en agosto de 2021 y no corresponde al monto equivalente en el momento de la contratación.

14 Ver https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d y https://www.hrw.org/es/news/2020/10/09/argentina-publica-en-linea-datos-personales-de-ninos-y-ninas-acusados-de-cometer

15 Ver https://realpolitik.com.ar/nota/37024/larreta-le-dio-el-control-del-reconocimiento-facial-a-una-empresa-denunciada-por-espiar-a-cfk/

16 Ver https://www.eltribuno.com/salta/nota/2021-5-9-1-45-0-el-sistema-de-camaras-cuesta-mas-de-440-mil-dolares-por-mes

En el caso de la municipalidad de Tigre, la empresa NEC Argentina SA obtuvo la adjudicación de una licitación pública para proveer una "Plataforma Integral de Seguridad" en 2018 y nuevamente en 2019, esta vez bajo el concepto de "Adquisición de tótems de seguridad inteligente". En 2020, la empresa resultó adjudicada en una nueva licitación pública por "servicio de mantenimiento de sesenta (60) unidades de Tótems de Seguridad Inteligente (TSI)". En Argentina, el grupo de origen japonés NEC Corporation se encuentra establecido desde 1978 y desde entonces obtuvo múltiples contratos con el Estado.

Morpho Safran, ahora denominada IDEMIA, y DATYS son las proveedoras del Sistema Federal de Identificación Biométrica para la Seguridad, SIBIOS. La primera es una multinacional francesa dedicada al desarrollo de tecnologías, principalmente enfocado en la venta de productos de reconocimiento facial. La empresa ha sido criticada por Amnistía Internacional por exportar tecnologías de vigilancia digital a China, debido al riesgo a los derechos humanos implicado.[17] IDEMIA fue culpada por problemas con la elección general en Kenia en 2017, lo que resultó en que la Asamblea Nacional cancelara sus contratos vigentes y le prohibiera suscribir nuevos. La decisión fue derogada por la Corte Suprema del país.[18]

DATYS, por su vez, es una empresa cubana fundada en 2005. Según información obtenida por la Asociación por los Derechos Civiles (ADC), la herramienta contratada de DATYS permite la identificación automática de personas mediante la comparación de huellas digitales y, como método secundario, de rostros.[19]

Brasil

En Brasil fueron identificadas seis iniciativas de uso de sistemas de reconocimiento facial con los siguientes proveedores de tecnologías involucrados:

- Admobilize, de Estados Unidos, contratada para el desarrollo de tecnologías en un sistema de reconocimiento facial y de emociones instalado en las estaciones de metro del consorcio ViaQuatro, en la ciudad de São Paulo, activo entre marzo y septiembre de 2018.
- Staff of Security Technologies do Brasil Software Ltda, empresa brasileña que importó el software Facewatch desde Inglaterra para implementar un sistema de identificación facial en la edición de 2019 de la tradicional fiesta de San Juan, que ocurre anualmente en la ciudad de Campina Grande, provincia de Paraíba.
- Brisanet Telecomunicações, empresa brasileña que ofreció infraestructura para el sistema implementado en la fiesta de San Juan en Campina Grande en 2019.
- Tecway, empresa brasileña adjudicada en un proceso de licitación para el desarrollo de tecnologías biométricas para el Centro Integrado de Cámaras de Monitoreo de Itacoatiara, provincia de Amazonas, actualmente en proceso de implementación.
- Engie Brasil Soluções Integradas Ltda., empresa brasileña miembro del consorcio Engie Ineo Jonhson, adjudicado para la implementación de un sistema de reconocimiento facial en el metro de la ciudad de São Paulo en 2019.

---

17 Amnistía Internacional, "Out of control: failling EU laws for digital surveillance export" (2020). Ver https://www.amnesty.org/en/documents/eur01/2556/2020/en/

18 Ver https://www.biometricupdate.com/202101/criticism-sparked-by-delay-of-biometric-election-systems-unveiling-in-uganda-procurement-in-kenya

19 Asociación por los Derechos Civiles, "La identidad que no podemos cambiar: cómo la biometría afecta nuestros derechos humanos" (2017), ver https://adc.org.ar/wp-content/uploads/2019/06/027-A-la-identidad-que-no-podemos-cambiar-04-2017.pdf. Y "Tu yo digital – Descubriendo las narrativas sobre identidad y biometría en América Latina: los casos de Argentina, Brasil, Colombia y México" (2019), ver https://adc.org.ar/wp-content/uploads/2020/06/050-tu-yo-digital-04-2019.pdf

- Ineo Infracom, empresa francesa miembro del consorcio Engie Ineo Jonhson adjudicado para la implementación de un sistema de reconocimiento facial en el metro de la ciudad de São Paulo en 2019.
- Johnson Controls BE do Brasil Ltda, empresa estadounidense miembro del consorcio Engie Ineo Jonhson adjudicado para la implementación de un sistema de reconocimiento facial en el metro de la ciudad de São Paulo en 2019.

En el caso de Campina Grande, las tecnologías fueron obtenidas por medio de una donación de las proveedoras a la empresa Medow Entertainment, responsable de la organización de la fiesta de San Juan en 2019. La empresa Staff of Security Technologies do Brasil Software Ltda, responsable de la importación del software Facewatch tiene vínculos con una figura política involucrada en varios escándalos de corrupción a nivel nacional.[20]

Según informaciones de Privacy International, la empresa Facewatch tendría distribuidores locales tanto en Brasil, como en Argentina. En Reino Unido, sus sistemas han sido adoptados por distintos tipos de comercios con la finalidad de identificar personas consideradas no deseables en ese tipo de negocio (por comportamientos antisociales, intentos de hurtos, etc.) y su inclusión en una lista negra. Al pasar por una cámara para ingresar al negocio o evento, el sistema identifica si la persona está o no en la lista y, en caso positivo, envía una alerta. El sistema ha generado polémica en el país con relación a la legalidad de su uso y las implicaciones a la privacidad, según informa la BBC.[21]

De acuerdo con Privacy International, en 2019 el sistema de Facewatch era utilizado en al menos tres centros comerciales en Brasil. A propósito de una investigación sobre una posible colaboración entre la empresa y la policía de Londres para el intercambio de datos, la organización alerta sobre la anunciada intención del gobernador de Río de Janeiro de permitir a la policía local intercambiar su propia lista de personas sospechosas de cometer crímenes con empresas de reconocimiento facial.[22]

Por su parte, la empresa brasileña Tecway, contratada para desarrollar el Centro Integrado de Cámaras de Monitoreo de Itacoatiara, tiene entre sus antecedentes una investigación del Ministerio Público de la provincia de Amazonas debido a posibles ilicitudes en una licitación pública y una cita por parte de la comisión instalada en el Senado brasileño para investigar irregularidades durante la gestión de la pandemia de Covid-19.[23] Uno de los socios de la empresa es familiar de un diputado nacional e intentó presentarse como candidato a un puesto local en Manaus, capital de Amazonas.[24]

Dos iniciativas cuentan con servicios de la proveedora pública de tecnología: el Servicio Federal de Processamento de Datos (SERPRO), que ofrece la base y el almacenamiento de los datos biométricos. SERPRO está involucrado en la implementación de la validación de la licencia nacional de conducción por medio de datos biométricos y para las "pruebas de vida", un requisito anual obligatorio para que no haya interrupción en el pago de las pensiones por el sistema de seguridad social brasileño. En este caso, el objetivo es reemplazar el proceso en persona por

---

20 Ver https://agenciasportlight.com.br/index.php/2019/06/11/o-governador-witzel-e-as-caras-ocultas-no-milionario-negocio-de-reconhecimento-facial/

21 Ver https://www.bbc.com/news/technology-55259179

22 Ver https://privacyinternational.org/long-read/4216/facewatch-reality-behind-marketing-discourse

23 Ver https://amazonasatual.com.br/promotora-chama-de-esdruxula-forma-como-ssp-am-iniciou-negocio-de-r-427-milhoes-para-aluguel-de-viaturas-2/ y https://www.metropoles.com/colunas/igor-gadelha/cpi-pede-quebra-de-sigilo-de-empresa-de-parente-do-lider-do-mdb

24 Ver https://simenao.com.br/simenao/autor-de-post-que-viralizou-teve-candidatura-indeferida-pela-ficha-limpa

una app, donde la beneficiaria envía una "selfie" que es comparada con la foto registrada en las bases de datos del sistema.

SERPRO es una empresa pública vinculada al Ministerio de Hacienda y su objeto es ejecutar servicios de procesamiento de información y datos, incluyendo las actividades de teleprocesamiento y comunicación de datos, voz e imagen que se requieran, de manera limitada y especializada. El máximo órgano director de SERPRO es la Junta Directiva integrada por seis miembros nombrados por el Presidente de la República y recomendados por el Ministro de Estado de Hacienda.
Dos iniciativas recientes cuestionan en el Poder Judicial el uso indebido de datos almacenados por el SERPRO. La primera solicita la suspensión del intercambio de datos con la Agencia Brasileña de Inteligencia (ABIN).[25] La segunda cuestiona la legalidad del uso de la base de datos de las licencias de conducir para la oferta de servicios de reconocimiento facial para el sector público y privado.[26]

Chile

En Chile, si bien se identificaron diez iniciativas de uso de sistemas de reconocimiento facial desde el sector público, de las cuales seis se encuentran activas, no fue posible identificar los proveedores involucrados en su despliegue, en general debido a la lentitud en la respuesta de los órganos públicos a las solicitudes de acceso a la información presentadas a propósito de esta investigación.

Únicamente en el caso de la municipalidad de San Joaquín se pudo identificar las empresas Enel Distribución Chile SA y Sistema de Seguridad y Tecnologías SpA como adjudicadas en una licitación pública publicada en 2019 para el mejoramiento del sistema de televigilancia de la municipalidad.[27] El monto ofrecido por los trabajos contratados fue de 789.888.183 pesos chilenos (CLP), el equivalente al día de hoy a alrededor de 1.023.965 dólares.

Enel Distribución Chile SA fue contratada para el servicio de proveer "sistemas de control o vigilancia de potencia". La empresa es parte del Grupo Enel, multinacional de origen italiano, responsable por la distribución de electricidad en varias localidades del país, pero ha ingresado al negocio de las cámaras de seguridad en 2018.

Colombia

En Colombia fueron identificadas cinco iniciativas de uso de sistemas de reconocimiento facial, en los cuales los siguientes proveedores se encuentran involucrados:

- La empresa de servicios públicos mixta colombiana EMTEL, contratada a través de un convenio interadministrativo por parte de la Alcaldía de Bogotá por 11.758.251.357 COP (aproximadamente 3.100.000 USD) suscrito en 2015, para reunir los esfuerzos necesarios para la puesta en funcionamiento del Sistema Integrado de Videovigilancia Inteligente para Transmilenio (SIVIT), desactivado en 2021.
- Inversiones Tecnológicas de América, también colombiana, subcontratada por EMTEL para el suministro de equipos que permitieran el funcionamiento del SIVIT: cámaras,

25 Ver https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/ y https://www.jota.info/stf/do-supremo/psb-aciona-stf-contra-compartilhamento-de-dados-da-cnh-entre-serpro-e-abin-16062020

26 Ver https://computerworld.com.br/plataformas/ministerio-publico-acusa-serpro-de-oferecer-servico-ilegal/

27 Ver https://www.mercadopublico.cl/Procurement/Modules/RFB/DetailsAcquisition.aspx?qs=/qaUKJpnZ48L4Wt-kI40xyg==.

iluminación, switches y pantallas, entre otros.

- Compañía Internacional de Integración S.A. y TecniDidácticos IND S.A.S (Unión Temporal Tecnocom), colombiana, contratada por COP 11,298,307,350.00 (aproximadamente 2.865.268 USD) para liderar la implementación del Sistema Multibiométrico ABIS de la policía nacional y el Ministerio del Interior, activo desde 2017.
- IDEMIA, empresa francesa, subcontratada por la anterior para el desarrollo de los registros dactilares del sistema y la migración del sistema utilizado anteriormente por la policía para el ABIS. El valor del contrato fue de 1.000.000.000 COP (253.603 USD aproximadamente). La misma empresa está involucrada en la implementación de la "Cédula de identidad digital", especificamente del motor multibiométrico Morpho Biometric Search Service.[28]
- HERTA Security, española, también subcontratada por la Unión Temporal Tecnocom para migrar fotografías para la base de datos digital e instalar sus aplicativos en el sistema ABIS (Biodata, BioFinder y Biogenerator).
- Empresa de Telecomunicaciones de Bogotá, empresa pública colombiana encargada de desarrollar pruebas de implementación en cámaras de reconocimiento facial de la Agencia de Analítica de Datos (Ágata) de Bogotá, activa desde 2020.
- BYTTE SAS, colombiana, adjudicada en una licitación pública con el valor de 13.994.000.000 COP (3.549.058 USD aproximadamente) para liderar el despliegue del Sistema integrado de información Multibiométrico actualmente en proceso de implementación.

La imposibilidad de activar las cámaras de reconocimiento biométrico previstas en el SIVIT y contratadas con EMTEL llevaron a que la personería de Bogotá investigara a dos subgerentes del Fondo de Vigilancia y Seguridad de esa ciudad.[29] Aunque la investigación se cerró en 2021, [30]se formularon cargos contra los ex subgerentes por negligencia en la contratación, ya que no tomaron en consideración las advertencias de que tal sistema solo podría operar en caso de que contara con una base de datos fotográfica que no existía.

En 2019 el alcalde de Popayán y el exsecretario de Tránsito Municipal fueron investigados por posibles actos de corrupción, como la entrega irregular de los servicios de tránsito a una firma denominada Quipux por medio de Emtel.[31]

La Unión Temporal Tecnocom, a su vez, enfrentó cuatro procesos en 2017 por presuntos incumplimientos en el desarrollo del contrato que se estableció con la Policía Nacional para el desarrollo del sistema ABIS. Las decisiones fueron favorables a la empresa. Tanto TecniDidácticos como la Compañía Internacional de Integración S.A. han celebrado varios contratos con el Estado colombiano. La francesa IDEMIA, por su parte, es la empresa con la que contrata la Registraduría Nacional del Estado Civil desde hace más de 10 años. TecniDidácticos es investigada desde 2020 por presuntas irregularidades en un contrato con la Alcaldía de Medellín para el suministro de tapabocas N95 durante la pandemia de Covid-19.[32]

En el caso de Ágata, son varios los inversionistas y facilitadores de la iniciativa, entre los cuales se encuentran la empresa de Acueducto de Alcantarillado de Bogotá, el Grupo de Energía de Bogotá, la Unidad Administrativa Especial de Catastro Distrital, la Secretaría Distrital de Planea-

---

28 Ver https://www.idemia.com/mbss

29 Ver https://www.personeriabogota.gov.co/sala-de-prensa/notas-de-prensa/item/578-inhabilitado-exsubgerente-de-fondo-de-vigilancia-y-seguridad

30 Secretaría de Seguridad, Convivencia y Justicia, "Cierre de investigación disciplinaria del proceso 015-2019". 04 de enero de 2021, Disponible en: https://scj.gov.co/sites/default/files/notificaciones_control_interno_disciplinario/ESTADO%20001%20Firmado%7D.pdf

31 Ver https://caracol.com.co/emisora/2019/01/29/popayan/1548787323_962726.html

32 Ver https://www.kienyke.com/crimen-y-corrupcion/denuncias-corrupcion-contratos-coronavirus-alcaldia-medellin

ción, Transmilenio S.A. y la Empresa Metro de Bogotá. Sin embargo, la Empresa de Telecomunicaciones de Bogotá (ETB) tiene una participación mayoritaria del 51% en la Agencia. Además, lideró su proceso de conformación junto con entidades de la Alcaldía de Bogotá.[33] La empresa cuenta con varios contratos con diversas instituciones públicas en la ciudad de Bogotá.

La ETB fue sancionada por violar el derecho a la libre elección a sus usuarios por no atender la terminación de contratos en los plazos establecidos y estuvo involucrada en algunas irregularidades relacionadas a incumplimientos en la ejecución de contratos.[34]

Finalmente, Bytte S.A.S ha tenido contratos tanto con entidades públicas como privadas para la adecuación de softwares de control de acceso y soporte a sistemas de carnetización. Las clientes incluyen la Aeronáutica Civil y la Universidad Pedagógica y Tecnológica de Colombia, sede Tunja. En 2010 la empresa desarrolló una alianza con Safran Morpho, hoy IDEMIA.[35]

Costa Rica

Se han identificado en Costa Rica tres iniciativas que involucran el uso de sistemas de reconocimiento facial. La francesa IDEMIA —que cuenta con una fábrica en Costa Rica — fue contratada junto a un consorcio por medio de una licitación en el valor de 3.674.203 USD para el desarrollo del software utilizado en el Sistema de Identificación Biométrica Automatizada (ABIS) que incluye distintos elementos de identificación biométrica, incluyendo el reconocimiento facial.[36] El sistema se implementó a fines de 2020, con énfasis particular en emisión de cédulas y de tarjetas de identidad a personas menores de edad (12 a 18 años).

También integra el consorcio IAFIS, empresa creada en Argentina para la venta de sistemas de Morpho (actual IDEMIA) en América Latina.[37] La involucrada en ABIS y miembro del consorcio es Componentes El Orbe S.A, empresa costarricense con actuación en distintos países de Centroamérica. Todas las involucradas en el contrato han trabajado en otros proyectos con el Estado de Costa Rica. En el caso de IAFIS, es la responsable del Sistema Automatizado de Identificación de Huellas Dactilares del Tribunal Supremo de Elecciones.

En el caso del Sistema Migratorio de Identificación Biométrica, en proceso de implementación, en febrero de 2020 se cerró el periodo de recepción de ofertas en el marco de la licitación abierta para la contratación. El presupuesto estimado es de 3.317.389.479,96 CRC (equivalente a alrededor de 5.344.276,41 USD). Según el sistema de compras públicas, la adjudicación todavía está en evaluación. Sin embargo, de acuerdo con la Dirección General de Migración y Extranjería, el proyecto se adjudicó al consorcio GSI-Dinámica-Veridos-Sertracen. Tanto el Grupo de Soluciones Informáticas SA (GSI) como Sertracen son empresas con una relevante presencia en Centroamérica.

---

33 Ver https://www.valoraanalitik.com/2020/12/14/bogot-lanza-gara-nueva-agencia-de-anal-tica-de-datos/ https://bogota.gov.co/mi-ciudad/administracion-distrital/que-es-la-agencia-analitica-de-datos-de-la-alcaldia-de-bogota y https://gestor.etb.net.co/mp4/ABECE.pdf

34 Ver https://www.eltiempo.com/bogota/sancion-superintendencia-de-industria-y-comercio-impone-millonaria-sancion-a-la-etb-522846

35 Ver https://repository.urosario.edu.co/bitstream/handle/10336/13091/PedrozoBoada-MullerJose-2017.pdf?sequence=1&isAllowed=y

36 El contrato puede encontrarse en https://www.sicop.go.cr/moduloPcont/pcont/ctract/es/CE_COJ_COQ038_O.jsp?contract_no=CE201905000256&contract_mod_seq=00&typeExp=Y

37 Ver https://www.linkedin.com/company/iafisgroup/about/

El consorcio también fue beneficiado con la contratación para la implementación del Pasaporte Biométrico para el Bicentenario, que tiene previsto integrar el reconocimiento facial como mecanismo de autentificación hasta marzo de 2022. En ese caso, el valor del contrato fue de 5.501.308,159 USD. El consorcio incluye a Dinámica Consultores Internacional S.A, también de Costa Rica, y Veridos de Alemania.

México

En México fueron identificadas tres iniciativas de implementación de sistemas de reconocimiento facial para la vigilancia de espacios públicos. Las proveedoras involucradas son las siguientes:

- Dahua, empresa de origen chino, contratada por medio de una adjudicación directa en el valor de 600 millones MXN (aproximadamente 29.494.148 USD) para la implementación y manutención del Sistema de Video-Inteligencia del Estado de Coahuila. Actualmente en etapa piloto, la iniciativa implica la instalación de 300 cámaras de vigilancia con capacidad de reconocimiento facial en 11 ciudades del Estado.
- La empresa mexicana Teléfonos de México S.A.B. de C.V. fue adjudicada en una licitación pública nacional en el valor total de 197.564.863,80 MXN (alrededor de 9.702.029 USD) para la implementación del Centro de Comando y Control C2 de la Central de Abastos de la Ciudad de México de la Central de Abastos de la Ciudad de México.
- En la misma licitación han sido también contratadas Hanwa, de Corea del Sur, para el desarrollo de tecnologías biométricas; y la empresa de ingeniería estadunidense Intelligent Security Systems, también dedicada al desarrollo de tecnologías biométricas.
- Compañía SYM Servicios Integrales, S.A. de C.V., de México, fue contratada por un valor total de 728.010.176 MXN (36.118.859 USD aproximadamente) para la implementación y manutención del Centro de Comando, Control, Comunicación, Cómputo y Coordinación "C5 SITEC' – activo desde mayo de 2021. La iniciativa incluye la instalación de 40 cámaras con capacidad de reconocimiento facial, instaladas en 20 puntos del municipio de Aguascalientes en el estado del mismo nombre.

Con relación al Sistema de Video-Inteligencia de Coahuila, Dahua ha declarado a la prensa que los algoritmos provistos han sido "tropicalizados" para identificar el "fenotipo mexicano", lo que sugiere que la empresa tuvo alguna posibilidad de acceso a datos de personas mexicanas para el entrenamiento de sus sistemas de reconocimiento facial. La iniciativa fue presentada al público poco tiempo después de una visita del gobernador de Coahuila a China, en que se reunió con la empresa. Durante el lanzamiento del sistema estuvo presente su CEO, Zhijie Li.

La empresa, una de las más importantes en el mercado global de videovigilancia, ha sido sancionada por Estados Unidos en 2019 por violaciones de derechos humanos debido a su participación en campañas de hostigamiento en contra de una minoría islámica.[38] La empresa mantiene contratos para proyectos de vigilancia en Xinjiang, donde el gobierno chino es acusado de genocidio a la población Uighur. Según informaciones publicadas por la prensa estadounidense a principios de 2021, su software de reconocimiento facial sería capaz de identificar personas de tal etnia.[39]

Hikvision, una de las adjudicadas en el Proyecto de Videovigilancia Urbana Integral con Tecnología Analítica, fue sancionada por Estados Unidos en 2019 y por Noruega en 2020 por abusos

38 Ver https://www.icij.org/investigations/china-cables/us-blacklists-chinese-companies-linked-to-uighur-abuses/

39 Ver https://www.latimes.com/business/technology/story/2021-02-09/dahua-facial-recognition-china-surveillance-uighur

a derechos humanos.[40] Sus tecnologías de vigilancia también serían utilizadas por el gobierno chino para reprimir a personas de minorías musulmanas.

La mexicana Teléfonos de México, por su vez, se ha encargado de la gran mayoría de los proyectos relacionados con la instalación de cámaras de vigilancia en la Ciudad de México. Dicha empresa es propiedad de Carlos Slim el cual ha ganado proyectos millonarios, y ha tenido una importante participación en proyectos de infraestructura en las últimas tres administraciones de la Ciudad de México. En uno de los proyectos con participación de la empresa se han encontrado diversas irregularidades como pagos injustificados, la falta de comprobación de gastos, facturas extraviadas, entre otros.[41]

En el caso de Aguascalientes, la forma de contratación mediante adjudicación directa podría ser violatoria de lo establecido en la Ley De Adquisiciones, Arrendamientos y Servicios del Estado de Aguascalientes. En el contrato declaran que se sustenta en las fracciones I y VII del artículo 63 de dicha Ley, los cuales establecen que se podrá hacer adjudicación directa si no hay servicios o bienes sustitutos o equivalentes a los ofertados por la empresa o si bien el realizar otro tipo de procedimiento de contratación pueda comprometer información de carácter confidencial y/o reservada. Sin embargo, iniciativas equivalentes han sido contratadas mediante licitaciones públicas, lo cual apoya al hecho de la posible violación de lo establecido en la referida ley.

La contratada, SYM Servicios Integrales, tiene una larga historia en aprovisionamiento gubernamental en el rubro de sistemas y equipos de seguridad, entre sistemas de videovigilancia del espacio público y sistemas de vigilancia.[42] De acuerdo a correos filtrados por Wikileaks, la empresa ha vendido sistemas de vigilancia fabricados por la empresa Hacking Team a gobiernos locales en México (entre ellos los de Tamaulipas, Campeche, Puebla y Jalisco). SYM Servicios Integrales S.A. de C.V. es una de las filiales de Grupo Kabat, que también comercializa sistemas de Hacking Team a gobiernos de otros estados en México. Según el New York Times, dichos sistemas fueron utilizados por el gobierno de Puebla para espiar a contrincantes políticos en el contexto electoral.[43]

Panamá

En Panamá fueron mapeadas tres iniciativas de uso de reconocimiento facial en las cuales están involucradas dos empresas extranjeras. Una de ellas es Huawei Technologies, contratada para el desarrollo de tecnologías biométricas para el Centro de Operaciones de Seguridad y Emergencias C2, iniciativa que se encuentra activa desde 2018. El valor de la contratación, 9,3 millones de dólares estadounidenses, se pagó por medio de un préstamo no reembolsable de China, lo que significa que los servicios fueron donados por el gobierno chino al país. Cabe señalar que Huawei Technologies mantiene una sociedad anónima que representa sus intereses en Panamá, todas las personas en su Junta Directiva son ciudadanos chinos y no habitan en Panamá.

La otra empresa involucrada en la provisión de tecnologías biométricas en Panamá es la canadiense General Dynamics Mission Systems, contratada para el Proyecto de Reconocimiento Facial Biométrico del Aeropuerto de Tocumen y el Paso Centro de Operaciones Nacionales, ambas activas desde 2019. Los contratos alcanzaron el valor de 4.786.388 y 27,5 millones de USD,

40 Ver https://www.dw.com/en/us-blacklists-28-chinese-companies-over-xinjiang-rights-abuses/a-50732014

41 Ver https://poderlatam.org/2020/01/el-negocio-de-slim-en-el-centro-historico-de-la-cdmx/

42 Ver https://www.quienesquien.wiki/es/empresas/sym-servicios-integrales-sa-de-cv?collection=all&name=SYM+-SERVICIOS+INTEGRALES+SA+DE+CV&tipo-entidad=&pais=&estado=&ciudad=&fuente=&size=&sort-all=#summary-supplier_contract.

43 Ver https://r3d.mx/2017/01/05/nyt-documenta-uso-de-malware-para-espionaje-politico-en-puebla/

respectivamente. La empresa mantiene distintos contratos con el gobierno panameño en el marco de una cooperación del país con la Cámara Comercial Canadiense.

Paraguay

En Paraguay fueron identificadas tres iniciativas de uso de reconocimiento facial. En todas están involucradas dos proveedoras nacionales responsables por la implementación y mantenimiento de los sistemas. La primera es Tecnología, Seguridad y Vigilancia del Paraguay S.R.L, contratada a partir de una licitación en valor de 3 millones de USD en el marco del proyecto de reconocimiento facial en espacios públicos urbanos que actualmente se encuentra implementado en Asunción, Encarnación, San Ignacio, Caaguazú, Coronel Oviedo y Ciudad del Este. La empresa provee servicios para la policía de Paraguay al menos desde 2011 según la prensa local, que también ha levantado dudas con relación al efectivo funcionamiento de las tecnologías de reconocimiento facial desplegadas.[44]

La también paraguaya Asunción Comunicaciones S.A., fue adjudicada en una licitación para la Ampliación de Capacidades, Garantías y Facial del Sistema AFIS (*Automated Fingerprint Identification System*). El contrato ha resultado en 1.676.303 de USD en ingresos en 2017 y 1.813.215 en 2019. Como parte del servicio, la empresa ha provisto licencias de softwares biométricos para móviles, licencias de Middleware central biométrico móvil, licencia registrada AFIS criminal, licencia de actualización de software central facial y licencia de actualización estación de trabajo de software facial.

Asunción Comunicaciones S.A. también ha sido adjudicada en una licitación pública para la implementación del Sistema AFIS en un evento deportivo, como parte de una acción conjunta con la Asociación Paraguaya de Fútbol y la Policía Nacional, liderado por el Ministerio del Interior. La acción piloto realizada en 2019 resultó en una inversión de 1.642.093 USD aproximadamente.

Perú

En Perú fue identificada una única iniciativa de implementación de sistemas de reconocimiento facial en Gamarra, uno de los centros comerciales más importantes del país, ubicado en la región metropolitana de Lima. El sistema se encuentra en proceso de implementación desde 2019. La iniciativa contó con la participación de la empresa peruana Desarrollos Terrestres, encargada de la instalación de cámaras.

El mecanismo de contratación en este caso es particular: la empresa Desarrollos Terrestres ha ido celebrando convenios con distintas municipalidades distritales en Lima. Así, según estos convenios, la empresa se obligaba a instalar las cámaras y brindar un sistema de monitoreo a la Municipalidad. A cambio de ello, la Municipalidad se comprometía a facilitar la instalación de redes de telecomunicaciones en el distrito.

44 Ver https://www.abc.com.py/edicion-impresa/economia/2019/11/11/tsv-srl-es-la-eterna-proveedora-tecnologica-del-911-de-la-policia/

A modo de conclusión: el reconocimiento facial no nos protege, nos vulnera

Distintos gobiernos alrededor del mundo han comenzado a imponer prohibiciones y moratorias a la implementación y uso del reconocimiento facial y algunas empresas desarrolladoras de software se han comprometido con la restricción de ventas de este tipo de sistemas en determinadas situaciones. Es el caso de Amazon,[45] Microsoft[46] e IBM,[47] que se manifestaron expresamente en ese sentido tras los episodios de protestas por justicia racial en Estados Unidos en 2020. Estas manifestaciones se producen al mismo tiempo que se descubren sesgos raciales en estas tecnologías.[48]

Expertos y expertas internacionales también se han posicionado de manera favorable a la imposición de este tipo de medida,[49] considerando que los sistemas de reconocimiento facial implican una serie de impactos al ejercicio de los derechos humanos.[50]

¿Por qué no? Afectación a los derechos humanos y riesgos asociados al uso de reconocimiento facial

Cabe recordar que la tecnología de reconocimiento facial permite la identificación individualizada de cualquier persona y, con eso, el acompañamiento de sus trayectos y hábitos personales en tiempo real. La transformación de tal información en metadatos que pueden, a su vez, ser almacenados y analizados de manera agregada implica la posibilidad adicional de inferir una serie comportamientos e, incluso, intentar predecir acciones futuras.

Especialmente cuando son implementados en espacios públicos — como es el caso de la mayoría de las iniciativas identificadas a partir de este mapeo —, los sistemas de reconocimiento facial consisten en una tecnología de vigilancia masiva encubierta que afecta a todas las personas que circulan por determinado espacio, sin que tengan conocimiento o la posibilidad de consentir la recolección de información personal sensible, como sus datos biométricos. Eso incluye, por ejemplo, a niños, niñas y adolescentes (NNA), cuya privacidad goza de protección especial debido al enorme impacto que usos abusivos o filtraciones de esa información extremadamente sensible pueden tener al libre desarrollo de su personalidad. Organizaciones de sociedad civil han identificado la inclusión indebida de datos de menores a las bases de datos del Sistema de

45 El País. Amazon suspende indefinidamente la venta de su tecnología de reconocimiento facial a la policía. Ver https://elpais.com/tecnologia/2021-05-21/amazon-suspende-indefinidamente-la-venta-de-su-tecnologia-de-reconocimiento-facial-a-la-policia.html.

46 The Washington Post. Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM. Ver https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.

47 El País, IBM abandona la tecnología de reconocimiento facial por las dudas éticas sobre su uso. Ver https://elpais.com/tecnologia/2020-06-09/ibm-abandona-la-tecnologia-de-reconocimiento-facial-por-las-dudas-eticas-sobre-su-utilizacion.html.

48 Ver Buolamwini J.; Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research 81:1–15, 2018. Recuperado: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

49 Ver https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736

50 Moratorium call on surveillance technology to end "free-for-all" abuses: UN expert. En: UN News [Internet]. 25 de junio de 2019 [citado 18 de febrero de 2020]. Recuperado: https://news.un.org/en/story/2019/06/1041231

Reconocimiento Facial de Prófugos (SRFP) implementado en algunas estaciones de subte de la Ciudad Autónoma de Buenos Aires.[51]

La instalación de sistemas de reconocimiento facial para la vigilancia de espacios públicos, por lo tanto, implica necesariamente restricciones al derecho a la libre circulación, puesto que quien no quiera que el sistema recolecte sus datos biométricos tendría que buscar caminos o medios de transporte alternativos. Por otro lado, el grado de intrusión propio de este tipo de tecnología implica una vulneración al derecho a la privacidad y, de manera asociada, al derecho a la protección de datos personales.[52]

Además, las capacidades de monitoreo y predicción de comportamientos comprometen el ejercicio del derecho a la libre asociación, expresión y reunión pacífica, una vez que permiten el perfilamiento de participantes de movimientos que contraríen intereses políticos o económicos establecidos vulnerando su anonimato y facilitando la criminalización o persecución de expresiones legítimas de distinto carácter.[53] Más que un ejercicio imaginativo, se trata de un riesgo concreto en países marcados por un histórico de autoritarismo e innumerables ejemplos recientes de abusos, por ejemplo, en la vigilancia de opositores y opositoras políticas, como es el caso de la mayoría de los países analizados. La posibilidad de estar bajo vigilancia constante, además, incentiva el silenciamiento y la autocensura, y representa un riesgo gravísimo para las sociedades democráticas.

Las implicaciones de la vigilancia individualizada de personas en tiempo real no afecta solamente a las personas involucradas en la defensa de derechos humanos o distintas formas de activismo. En una región particularmente marcada por el racismo, el machismo y la homofobia de manera estructural, este tipo de sistema facilita la violencia sexual por parte de aquellas personas que tengan acceso a la operación del sistema. Si bien se espera que las operadoras estén sujetas a reglas y controles estrictos, no son raros los episodios de abusos y discriminación por parte de agentes policiales en la región.

El derecho a la no discriminación, reconocido en los artículos 1 y 24 de la Convención Americana sobre Derechos Humanos, también se ve directamente amenazado por las altas tasas de falsos positivos que arrojan los sistemas de reconocimiento facial, problema que aumenta exponencialmente cuando las personas que están siendo vigiladas pertenecen a grupos históricamente

---

51 Ver https://www.hrw.org/es/news/2020/10/09/carta-al-lic-horacio-rodriguez-larreta-sobre-el-sistema-de-reconocimiento-facial-de

52 Ver, por ejemplo: Asamblea General de las Naciones Unidas. 20 de noviembre de 2013. El derecho a la privacidad en la era digital. A/RES/68/167. Recuperado: https://undocs.org/pdf?symbol=es/A/RES/68/167 y Naciones Unidas, resolución del Consejo de Derechos Humanos, 'El derecho a la privacidad en la era digital', A/HRC/34/L.7/Rev.1, Naciones Unidas, Nueva York, 2017.

53 Ver Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Informe "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, 24 de junio 2020, párrafo 31, disponible en: https://undocs.org/es/A/HRC/44/24. Ver también: Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación, Informe Derechos a la libertad de reunión pacífica y de asociación, 17 de mayo 2019, párrafo 56, disponible en: https://undocs.org/es/A/HRC/41/41. Sobre las implicaciones de la vigilancia al derecho a la libertad de expresión ver: Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. Estándares para una Internet Libre, Abierta e Incluyente. OEA/Ser.L/V/II CIDH/RELE/INF.17/17. Organización de Estados Americanos; 2017 mar. Recuperado: http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf y Consejo de Derechos Humanos, Asamblea General de Naciones Unidas. El derecho a la privacidad en la era digital. A/HRC/28/L.27. Organización de las Naciones Unidas; 24 de marzo de 2015. Recuperado: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pdf.

vulnerados como mujeres, personas de piel oscura o personas trans.[54] Los sistemas implementados en la región ya han registrado errores que resultaron en graves consecuencias para las personas afectadas.

En el Sistema de Reconocimiento Facial de Prófugos (SRFP) implementado en la Ciudad Autónoma de Buenos Aires, en Argentina, hay registros de al menos dos casos de falsos positivos, uno de los cuales implicó la detención de una persona inocente por seis días.[55] Situaciones similares también fueron identificadas en Brasil,[56] donde organizaciones han denunciado que, de un total de 151 personas detenidas a raíz del uso de sistemas de reconocimiento facial, el 90% son afrodescendientes.[57]

La implementación de sistemas de reconocimiento facial conlleva, por lo tanto, la reproducción técnica de los sesgos de exclusión social y, cuando son utilizados con fines de vigilancia, amenaza el derecho a la dignidad, al debido proceso y la presunción de inocencia.

Finalmente, cuando es implementado como mecanismos de autenticación de identidad para condicionar el acceso a servicios públicos, el reconocimiento facial (así como otras tecnologías biométricas) puede representar una barrera al ejercicio de derechos económicos y sociales. Además, implica que algunas personas, principalmente las que dependen de la asistencia social, están sujetas a garantías inferiores en términos de la protección de sus derechos fundamentales. Cuando son aplicadas de esta manera, las tecnologías refuerzan y profundizan las desigualdades estructurales históricas que afectan a la región.[58]

De la falta de transparencia pública a la resistencia ciudadana

Por todos los motivos aquí expuestos, es crucial que las decisiones asociadas a la implementación de sistemas de reconocimiento facial estén sujetas a estrictos controles democráticos — que incluyen criterios de legalidad, necesidad y proporcionalidad — y de supervisión pública. Sin embargo, el presente mapeo realizado por las organizaciones miembro de Al Sur evidencia que tales criterios son escasamente respetados en América Latina.

En primer lugar, las implementaciones carecen de discusiones públicas previas a su implementación. En la mayoría de los casos, las iniciativas se dan a conocer por medio de notas de prensa en medios especializados y de circulación restringida, a partir de publicación en medios oficiales de procesos de compras públicas (especialmente cuando se realizan por medio de licitaciones públicas, lo que no siempre ocurre) o cuando ya hay registros de abusos u otros tipos de escándalos de corrupción. Más grave es que, incluso durante este proceso de investigación, se han registrado barreras al acceso a la información sobre esos sistemas.

En segundo lugar, solo en dos de las 38 iniciativas identificadas estuvo previsto algún mecanismo de participación pública previa a la implementación de las tecnologías. Cuando se trata de la realización de estudios previos de impacto a la privacidad o a los derechos humanos, nuevamente solo dos iniciativas los implementaron. Finalmente, solo en tres de las iniciativas está

54 Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Informe "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, 24 de junio 2020, párrafo 32, disponible en: https://undocs.org/es/A/HRC/44/24

55 Ver https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien

56 Ver https://gizmodo.uol.com.br/rio-de-janeiro-reconhecimento-facial-erra-mulher-detida/.

57 Ver https://reconocimientofacial.info/denuncian-sesgo-racial-en-tecnologias-de-reconocimiento-facial-brasilenas/.

58 Ver https://www.derechosdigitales.org/13900/vigilancia-control-social-e-inequidad/.

prevista la realización de una auditoría externa que ofrezca garantías mínimas de la adecuada implementación de los sistemas.

El contexto regional se complementa con regulaciones débiles en materia de protección de datos personales y acceso a la información pública, controles insuficientes tanto en gasto público como en la implementación de tecnologías, un historial de autoritarismo y desdén por los derechos humanos, alta inseguridad social, políticas de austeridad y la promesa eterna del desarrollo en la forma de importación de tecnología. El resultado es que América Latina se convierte en un campo fértil para la adopción del reconocimiento facial con fines múltiples y sin ningún tipo de resguardos, que permitan evitar un uso contrario a los principios democráticos que rigen cada uno de los países de la región.

Frente a tal situación, organizaciones de la sociedad civil han recurrido a la Justicia para obtener más información y cuestionar el despliegue de esos sistemas en sus países o ciudades, debido a los potenciales riesgos implicados. En Brasil, la justicia ha confirmado la ilegalidad de un sistema de cámaras de reconocimiento de emociones instalado en estaciones de metro.[59] La sentencia es resultado de una acción colectiva liderada por el Instituto Brasileño de Defensa del Consumidor (Idec). Además de la interrupción de la recolección de datos por medio del sistema, determinada ya en 2018,[60] se establece una indemnización de 100 mil reales por daños morales colectivos.[61] Actualmente se están desarrollando en São Paulo otras acciones para cuestionar la instalación de cámaras de reconocimiento facial en el transporte público.[62]

En Argentina hay actualmente dos causas judiciales en curso en contra del Sistema de Reconocimiento Facial de Prófugos: una Acción Declarativa de Inconstitucionalidad (ADI) contra el Gobierno de la Ciudad de Buenos Aires, interpuesta por la Asociación por los Derechos Civiles (ADC)[63] y un caso de amparo colectivo promovido por el Observatorio de Derecho Informático Argentino (O.D.I.A) que buscan interrumpir la iniciativa.[64] Además, recientemente se admitió una demanda de amparo contra la operación de sistemas con tecnología de reconocimiento facial en Coahuila, México.

En Perú, un conjunto de estudiantes ha presentado cuestionamientos a la obligatoriedad de uso de reconocimiento facial para la participación en un examen de admisión a una universidad pública.[65] Y en Paraguay, la organización TEDIC ha presentado una acción de inconstitucionalidad, cuestionando la declaración del Estado paraguayo de que informaciones relacionadas a la implementación de sistemas de reconocimiento facial en el país son de seguridad nacional y, por lo tanto, reservadas.

Frente a los intentos de los Estados de la región por ocultar, encubrir y omitir del debate público el incremento de las capacidades de vigilancia por medio de tecnologías de reconocimiento facial, sus fallas, incapacidades, negligencias y peligros, la sociedad civil resiste y denuncia sus ilegalidades y abusos. Este no es un problema técnico, es una discusión política sobre el tipo de

---

59 Ver https://idec.org.br/noticia/idec-obtem-vitoria-contra-reconhecimento-de-emocoes-no-metro-de-sp

60 Ver https://idec.org.br/noticia/justica-impede-uso-de-camera-que-coleta-dados-faciais-do-metro-em-sp.

61 Ver https://teletime.com.br/10/05/2021/justica-condena-viaquatro-por-reconhecimento-facial-de-passageiros-sem-consentimento/.

62 Ver https://reconocimientofacial.info/metro-tera-que-explicar-licitacao-de-cameras-de-reconhecimento-facial/.

63 Ver https://adc.org.ar/2019/11/06/el-reconocimiento-facial-para-vigilancia-no-pertenece-a-nuestro-espacio-publico/

64 Ver <https://amicus.odia.legal/

65 Ver <https://reconocimientofacial.info/peru-uso-de-reconocimiento-facial-en-examen-de-admision-a-universidad-publica-genera-cuestionamientos/

sociedad que queremos y el rol que las tecnologías deben tener en ellas: herramientas para el desarrollo integral de las personas y la sociedad en su conjunto o una forma de perpetuar las desigualdades sociales e históricas, por medio de un autoritarismo técnicamente asistido.

Esta es una batalla particularmente importante en América Latina, donde los derechos humanos y las nociones de dignidad y autonomía de las personas muchas veces son menoscabadas en función de los intereses de elites políticas y económicas, y donde la democracia debe estar constantemente resistiendo los embates producto de la corrupción y los abusos de poder. Frente a la opacidad que ampara el despotismo, exigimos transparencia; frente a las imposiciones arbitrarias, exigimos debate democrático y participación plural en los procesos de toma de decisiones respecto a la implementación de tecnologías invasivas como el reconocimiento facial. Frente al tecnosolucionismo ramplón, exigimos una perspectiva de derechos humanos amplia, robusta y sofisticada. Frente a las promesas de modernidad vacías, exigimos desarrollo y dignidad para todas las personas.

La depredación de los derechos fundamentales en aras de los intereses políticos y económicos que sustentan la implementación de los distintos sistemas de reconocimiento facial aquí listados requiere una respuesta enérgica por parte de la sociedad civil en contra de los Gobiernos que no parecen dispuestos a tratar la problemática con la seriedad necesaria. Esperamos que este reporte sirva como un insumo a la lucha que ya están dando distintas personas, en distintas locaciones de América Latina, así como un incentivo para la preparación de las peleas del mañana.

www.alsur.lat

AlSur