

INCLO

INTERNATIONAL NETWORK OF
CIVIL LIBERTIES ORGANIZATIONS

ENERO 2021



TE ESTÁN MIRANDO

RESISTENCIAS FRENTE A LAS VULNERACIONES DE DERECHOS POR
SISTEMAS DE RECONOCIMIENTO FACIAL EN EL MUNDO

ÍNDICE

Introducción	03
--------------------	----

01

Los SRF y el derecho a la libertad de expresión	05
--	-----------

1.1 El Tribunal de Apelaciones del Reino Unido declara ilegal el escaneo de rostros	07
---	----

02

Los SRF y el derecho a la igualdad y la no discriminación	08
--	-----------

2.1 Arresto y detención injustificados en EE. UU	10
--	----

2.2 Vigilancia en Cisjordania/Territorios Palestinos Ocupados	11
---	----

2.3 Temores de un apartheid basado en inteligencia artificial en Sudáfrica	12
--	----

03

Los SRF y el derecho a la libertad de reunión y asociación	13
---	-----------

3.1 Manifestantes bajo vigilancia en Moscú	15
--	----

3.2 Un método para disuadir a manifestantes en Colombia	16
---	----

04

Los SRF y el derecho a la privacidad	17
---	-----------

4.1 Uso encubierto por parte de la policía en Canadá	19
--	----

4.2 Arrestada por una orden judicial inválida en Argentina	20
--	----

4.3 Cámaras Hikvision en un hospital infantil en Irlanda	21
--	----

4.4 La discrecionalidad del servicio secreto en Hungría	22
---	----

4.5 Un sistema que ve a través de los tapabocas de COVID-19 en India	23
--	----

4.6 Planes frustrados para armar una “rueda de identificación perpetua” con SRF en Australia	24
---	----

4.7 SRF sin regulación a lo largo y ancho de Kenia	25
--	----

Conclusión	26
-------------------------	-----------

Notas finales	27
----------------------------	-----------

INTRODUCCIÓN

En todo el mundo, desde Delhi hasta Detroit, de Budapest a Bogotá, distintos sistemas de reconocimiento facial (SRF) están siendo rápidamente desplegados en espacios públicos y privados.

Para 2019, 64 de 176¹ países estaban usando sistemas de vigilancia de reconocimiento facial. En EE. UU., para 2016 más del 50% de los adultos estaban en una base de datos de reconocimiento facial de la policía².

Las fuerzas de seguridad dicen usar los SRF para hacer cumplir la ley. Por ejemplo, el FBI declaró ante el Congreso de EE. UU. que el reconocimiento facial “produce una potencial pista a investigar”³.

En general, los sistemas de vigilancia con esta tecnología funcionan ubicando una o más caras en una imagen en movimiento o estática de una cámara, antes de determinar rasgos faciales distintivos de esa imagen. El sistema compara esa imagen, sin consentimiento, con una base de datos existente o una “lista de personas bajo vigilancia” con imágenes extraídas de bases de datos de fotografías de identificación policial, en busca de una correspondencia. Otros sistemas de reconocimiento facial pueden examinar tendencias demográficas o realizar análisis de emociones escaneando multitudes, también sin consentimiento.

Es sabido que estos sistemas presentan sesgos étnicos, raciales y de género⁴ contra personas no blancas y mujeres. Esto significa que es más probable que los sistemas de reconocimiento facial utilizados por las fuerzas de seguridad identifiquen erróneamente a personas no blancas y mujeres que

a hombres blancos. Tales imprecisiones quedaron a la vista en 2019, cuando se dio a conocer que el sistema de la Policía Metropolitana de Londres (Reino Unido) tenía un porcentaje de error del 81%⁵. Las graves implicancias de tales imprecisiones y el subsiguiente efecto disuasivo sobre el ejercicio del derecho a la protesta se evidencian al considerar la vigilancia indiscriminada de las multitudes durante las manifestaciones. Por ejemplo, la policía en India usó SRF con bases de datos de registros de conducir y padrones electorales para “identificar” a 1.900 manifestantes⁶ durante las revueltas en Delhi de febrero de 2020.

La tecnología está en constante transformación y surgen serios problemas éticos sin importar cuán precisa se vuelva. Basta considerar cómo la empresa de vigilancia Hikvision fue criticada por presuntamente haber proveído equipamiento de SRF en Xinjiang, China, donde se está encerrando forzosamente a musulmanes uigures⁷ en centros de detención. Que una herramienta sea precisa no garantiza que sea ética.

En junio de 2020, el Consejo de Política Tecnológica para EE. UU. de la Association for Computing Machinery (Asociación de Maquinaria Computacional) declaró que estos sesgos son “científica y socialmente inaceptables”⁸. Encontró que ponen en peligro los derechos fundamentales de las individuos a la privacidad, el empleo, la justicia y la libertad personal. El Consejo hizo un llamado a que se suspendan inmediatamente todos los usos de SRF, afirmando que puede causar “profundas lesiones” a las vidas, medios de subsistencia y derechos fundamentales de las individuos y en particular los más vulnerables de la sociedad.

También hubo oposición a los SRF en otros lugares del mundo durante 2020. En el Reino Unido, el Tribunal de Apelaciones consideró ilegal el uso de SRF automatizados por la Policía de Gales del Sur⁹. En Canadá, Clearview AI, una empresa que hace scraping de imágenes de redes sociales¹⁰ y ofrece a sus clientes, incluyendo a fuerzas de seguridad, acceso a su base de datos, se retiró del país¹¹ luego de una investigación que inició el Comisionado para la Privacidad sobre el uso de la tecnología por parte de la policía. En Moscú, un grupo de manifestantes presentó una denuncia¹² ante el Tribunal Europeo de Derechos Humanos sobre el uso de SRF en manifestaciones en Rusia. Y en Israel, la negativa de la policía y el ejército de Israel a revelar el uso de SRF en ese país y en Cisjordania/Territorios Palestinos Ocupados (TPO) encontró resistencia por parte de una organización de derechos civiles¹³.

Este informe se enfoca en las múltiples formas en que el creciente uso de SRF afecta las vidas cotidianas de los ciudadanos de 13 países de las Américas, África, Europa, Asia y Australia. Estas historias de 13 organizaciones que integran la *International Network of Civil Liberties Organizations* (INCLCO) ilustran cómo la vigilancia puede discriminar e infringir una variedad de derechos, incluyendo el derecho a la privacidad y las libertades de expresión, asociación y reunión.

Cada historia es específica de cada país, pero, consideradas en su conjunto, revelan cómo esta forma dañina de vigilancia se ha generalizado y arraigado alrededor del mundo tanto en las esferas públicas como privadas. También ilustran colectivamente la necesidad de un debate público y democrático sobre el uso de estas tecnologías y de leyes sólidas para proteger a los ciudadanos.



Los SRF y

El derecho a la libertad de expresión

01

Los SRF y el derecho a la libertad de expresión

Olga Cronin, Irish Council for Civil Liberties

Los sistemas y algoritmos de reconocimiento facial en general escanean multitudes de manera indiscriminada en busca de capturar y detectar¹⁴ las características faciales de la mayor cantidad posible de personas, con el potencial de perfilar a individuos por su etnicidad, raza, nacionalidad, género u otras características.

Dada la recolección general que estos sistemas de reconocimiento facial hacen de estos datos especialmente sensibles en lugares y eventos específicos —como protestas, manifestaciones y eventos religiosos—, queda claro que esta práctica tiene el potencial para disuadir a las personas de expresar su opinión públicamente o que, en países con gobiernos autoritarios, podría llevar al arresto y enjuiciamiento de aquellos que elijan hacerlo.

La libertad de expresión está consagrada en el artículo 19 de la Declaración Universal de los Derechos Humanos¹⁵; el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos¹⁶; el artículo 9.2 de la Carta Africana de Derechos Humanos y de los Pueblos¹⁷; el artículo 10.1 del Convenio Europeo de Derechos Humanos (CEDH)¹⁸; el artículo 13.1 de la Convención Americana sobre Derechos Humanos¹⁹; y el principio 23 de la Declaración de Derechos Humanos de la ASEAN (Asociación de Naciones del Sudeste Asiático)²⁰.

En 2019, el Relator Especial sobre la libertad de opinión y de expresión de las Naciones Unidas, David Kaye,²¹ resaltó que no hay lugar donde el carácter intrusivo de las tecnologías de reconocimiento facial sea más claro que en China, donde supuestamente

se usan para seguir y controlar a unos 11 millones de uigures²², un grupo mayoritariamente musulmán de los cuales se cree que un millón se encuentran en campos de detención.

El potencial para vulnerar la libertad de expresión de los SRF fue objeto del destacado caso de Ed Bridges y la organización Liberty en el Reino Unido, en el que un manifestante inició acciones legales contra la policía de Gales del Sur después de que su cara fuera escaneada mientras compraba regalos para Navidad y, posteriormente, durante una manifestación.

El Sr. Bridges junto con Liberty, organización miembro de INCLO, cuestionaron la evaluación de impacto en la protección de datos (DPIA, por sus siglas en inglés) realizada por la policía, argumentando que la evaluación silenciaba algunos de los riesgos que corren los derechos que pueden ser vulnerados por estas tecnologías, entre ellos, el derecho a la libertad de expresión. El Tribunal de Apelaciones del Reino Unido decidió, finalmente, que la evaluación de impacto realizada por la policía no había considerado adecuadamente los riesgos²³.

Ignorar los riesgos al derecho a la libertad de expresión que representan los SRF implica ponernos en peligro.

Tal como determinó el Sr. Kaye en su informe al Consejo de Derechos Humanos de la ONU: “la interferencia con la privacidad mediante la vigilancia selectiva está diseñada para reprimir el ejercicio del derecho a la libertad de expresión”²⁴.

El Tribunal de Apelaciones del Reino Unido declara ilegal el escaneo de rostros

Hannah Couchman, Liberty

Qué

El Tribunal de Apelaciones del Reino Unido falló a favor de Ed Bridges, activista de derechos humanos, al declarar que el uso de sistemas automatizados de reconocimiento facial por la policía de Gales del Sur es ilegal. Este fue el resultado de las acciones legales emprendidas por el Sr. Bridges, representado por la organización Liberty, contra la policía de Gales del Sur, que había utilizado estas tecnologías para escanear su rostro en dos ocasiones, mientras hacía compras para Navidad en el centro de Cardiff el 21 de diciembre de 2017 y en una manifestación pacífica antiarmas el 27 de marzo de 2018.

DÓNDE CARDIFF, GALES

CUÁNDO 21 DE DICIEMBRE DE 2017 Y 27 DE MARZO DE 2018

Detalles adicionales

La policía en Gales del Sur escaneó aproximadamente 500.000 rostros usando sistemas automatizados de reconocimiento facial en unas 50 ocasiones en distintos eventos públicos, como parte de un proyecto piloto conocido como “AFR Locate”, entre marzo de 2017 y abril de 2019. El Sr. Bridges solicitó una revisión judicial de esta práctica con el fundamento de que esta tecnología, entre otras cosas, no era compatible con el derecho al respeto de la vida privada, recogido en el artículo 8 del Convenio Europeo de Derechos Humanos (CEDDH), ni con la legislación sobre protección de datos.

El tipo de tecnología que atañe a este caso extrajo caras capturadas en una transmisión en vivo desde una cámara y las comparó automáticamente con rostros incluidos en una lista de personas vigiladas por la policía. De no detectarse correspondencia, el software borra automáticamente la imagen facial capturada de la transmisión en vivo. Sin embargo, si se detecta una correspondencia, se alerta a un oficial de la policía, quien revisa las imágenes para determinar si es necesaria alguna intervención.



Esta tecnología es una herramienta invasiva y discriminatoria de vigilancia masiva. Hace ya tres años que la policía de Gales del Sur la viene usando contra cientos de miles de nosotros sin nuestro consentimiento y frecuentemente sin que lo sepamos. Todos deberíamos poder usar los espacios públicos sin ser sometidos a una vigilancia opresiva.

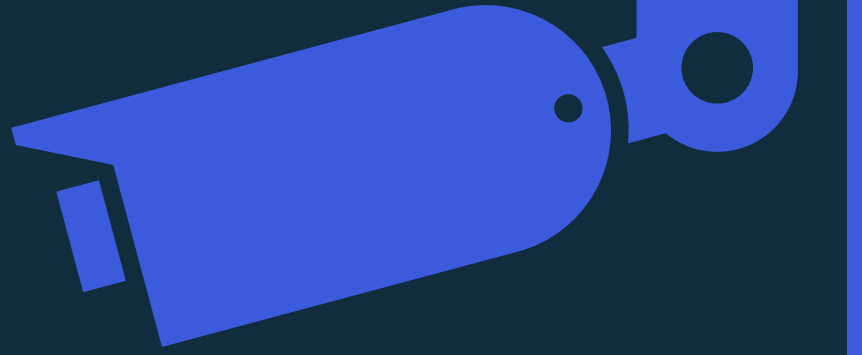
• ED BRIDGES, ACTIVISTA DE LIBERTADES CIVILES²⁵

Vulneraciones de derechos y libertades

En su fallo²⁶, el Tribunal de Apelaciones declaró que el uso de esta tecnología por parte de la policía era ilegal y que violaba el derecho a la privacidad y la ley sobre protección de datos. También encontró que la policía no investigó de manera independiente si la tecnología discriminaba por raza o sexo y si afectaba las leyes antidiscriminación. En concreto, el Tribunal declaró que no había fundamento legal suficiente para considerar acorde a derecho una práctica que vulnera el derecho a la privacidad, recogido en el artículo 8 del CEDH. La corte también encontró que la evaluación de impacto en la protección de datos llevada a cabo por la policía tampoco cumplía con la ley.

Acciones legales y de incidencia

Liberty representó al Sr. Bridges en el juicio. Megan Goulding, abogada de Liberty, dijo²⁷: “La corte concuerda en que esta herramienta distópica de vigilancia viola nuestros derechos y amenaza nuestras libertades... Es momento de que el gobierno [del Reino Unido] reconozca los serios peligros de esta tecnología invasiva. El reconocimiento facial es una amenaza a nuestra libertad; es necesario prohibirla”. Una petición de Liberty²⁸ reclamando que se prohíba el uso de SRF en espacios públicos fue firmada por más de 50.000 personas.



Los SRF y

El derecho a la igualdad y a la no discriminación

02

Los SRF y la discriminación

Gil Gan-Mor and Avner Pinchuck, Association for Civil Rights in Israel

El uso de SRF tiene el potencial real y significativo de reforzar y exacerbar las desigualdades estructurales y la discriminación. Estas vulneraciones pueden ser causadas principalmente por fallas en los algoritmos de la tecnología.

Las investigaciones hasta el momento indican que los SRF presentan sesgos contra las personas no blancas y las mujeres. En 2018, un estudio del MIT y la Universidad de Stanford evaluó programas de análisis facial de tres productores de SRF disponibles en el mercado. Encontraron errores en más de 20% de los casos relacionados con las caras de mujeres de piel oscura, lo que contrasta con una frecuencia de error de menos del 1% entre hombres de piel clara²⁹.

Otro estudio exhaustivo realizado en EE. UU. por el National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología)³⁰ encontró que la tecnología de reconocimiento facial tiene un sesgo significativo que lleva a la identificación errada en casos de personas de ascendencia africana y asiática.

También encontró que la mayor frecuencia de falsos positivos se da entre personas del este y oeste africano y personas asiáticas, y en menor medida entre personas del este de Europa; que la frecuencia de falsos positivos es más alta entre mujeres que entre hombres; y que hay elevados falsos positivos entre adultos mayores y niños.

Cuando una investigación policial se basa en esta tecnología, es probable que lleve a acusaciones e imputaciones erradas de manera desproporcionada entre determinados grupos.

Otra preocupación es el uso de tecnología para controlar y monitorear a las minorías, para sobrevigilarlas, poniendo cámaras conectadas con la tecnología en áreas identificadas con esos grupos minoritarios.

Arresto y detención injustificados en EE. UU.

Ben Wizner, American Civil Liberties Union

Qué

Robert Williams, residente de Detroit, fue arrestado luego de que el SRF usado por la Policía del estado de Michigan lo identificara erróneamente como un ladrón de relojes buscado. Los intentos del Sr. Williams y la American Civil Liberties Union (Unión Americana de Libertades Civiles) de conseguir detalles sobre los eventos que llevaron a su arresto han sido bloqueados³¹. El Departamento de Policía de Detroit admitió después que el sistema de reconocimiento facial que usa tiene un porcentaje de error del 96%³².

Detalles adicionales

En octubre de 2018, cinco relojes valorados en 3.800 dólares estadounidenses fueron robados de una tienda Shinola en Detroit. Más de un año después, el sistema de reconocimiento facial marcó una coincidencia errónea entre una imagen borrosa proveniente de la cámara de seguridad del negocio, en la que se ve al ladrón con una gorra de béisbol, y la foto de la licencia de conducir del Sr. Williams. Como resultado de ese grave error, el Sr. Williams fue esposado y arrestado en su casa, delante de su esposa y sus dos hijas³³, y permaneció detenido 30 horas. Fue subsiguientemente procesado por el delito de robo en primer grado y se le fijó una fianza de 1.000 dólares. Después de su arresto, el Sr. Williams fue llevado a un centro de detención donde la policía le tomó la foto para la ficha, huellas digitales y ADN antes de retenerlo durante la noche. En el interrogatorio del día siguiente, se hizo evidente que había sido arrestado por una identificación errada del sistema de reconocimiento facial. Los cargos fueron posteriormente retirados³⁴.

Vulneraciones de derechos y libertades

Lo que le ocurrió al Sr. Williams muestra cómo los SRF pueden llevar a errores de identificación, resultar en serias intromisiones en la privacidad, arrestos o detenciones erróneas y obstruir los principios y garantías del debido proceso y el juicio justo, es decir, del trato justo a les individuos.



Nunca pensé que tendría que explicarles a mis hijas por qué papá fue arrestado. ¿Cómo le explica uno a dos niñas pequeñas que una computadora se equivocó, pero la policía igualmente le hizo caso?

• ROBERT WILLIAMS

DÓNDE MICHIGAN, EE. UU.

CUÁNDO 9 DE ENERO DE 2020

Acciones legales y de incidencia

La ACLU de Michigan presentó una queja ante la ciudad de Detroit³⁵ que declara que el arresto por error del Sr. Williams “perturbó su vida familiar, resultó en su encarcelamiento injustificado y violó todas las normas de comportamiento policial e investigación razonables”. En particular, la carta reclamaba que el caso contra el Sr. Williams fuera desestimado; que el Sr. Williams recibiera una disculpa pública; que el Departamento de Policía de Detroit dejara de usar SRF como herramientas de investigación; que toda foto del Sr. Williams fuera borrada de cualquier base de datos policial de reconocimiento facial; y que la foto policial del Sr. Williams tomada después de su arresto fuera eliminada de todo archivo policial y estatal. Adicionalmente, la ACLU está ayudando a liderar una amplia coalición que puja por mayor supervisión y control comunitario³⁶ sobre la policía y el uso de tecnologías de vigilancia en Detroit³⁷.

Desde hace años, ACLU aboga por el fin del uso de tecnologías de reconocimiento facial por parte de los cuerpos de policía. En múltiples lugares, como San Francisco, Berkeley y Oakland en California, y Cambridge, Springfield y Somerville en Massachusetts, se ha prohibido que la policía use SRF. Amazon y Microsoft anunciaron recientemente que no venderán SRF a fuerzas policiales por un tiempo, pero aún no se han pronunciado³⁸ sobre la venta de la tecnología a fuerzas de seguridad federales como el FBI y la DEA (la Administración de Control de Drogas de EE. UU.).

Vigilancia en Cisjordania/Territorios Palestinos Ocupados

Gil Gan-Mor, Association for Civil Rights in Israel

Qué

Les palestines en Cisjordania/TPO que solicitan permisos para entrar a Israel deben dejar que les tomen una foto y las huellas digitales en una oficina militar israelí. Esas fotografías quedan guardadas en una base de datos biométricos y también se conectan con tarjetas de identificación electrónicas que tienen que escanear les palestines en puestos de control al entrar a Israel. Hasta agosto de 2019, 450.000 palestines, de les aproximadamente 2,7 millones de palestines que viven en Cisjordania/TPO, contaban con identificaciones electrónicas y sus fotos estaban registradas en la base de datos biométricos. Sus rostros son escaneados por sistemas de reconocimiento facial en los controles y se comparan con las fotos en la base de datos biométricos israelí.

DÓNDE CISJORDANIA/TPO

CUÁNDO DESDE 2018



Esta es una tecnología que, por su naturaleza, permite el seguimiento masivo de personas, no solo criminales, y tiene el potencial de dañar a todos.

- GIL GAN-MOR, DIRECTOR DE LA UNIDAD DE DERECHOS SOCIALES Y ECONÓMICOS DE LA ASSOCIATION FOR CIVIL RIGHTS IN ISRAEL³⁹

Detalles adicionales

Desde 2018, Israel ha estado usando reconocimiento facial en controles⁴⁰ en Cisjordania/TPO para verificar las identidades de palestines⁴¹ cuando entran a Israel. Los SRF no se usan en los controles para la población colona u otras personas de origen israelí que por trabajo cruzan diariamente la frontera entre Cisjordania/TPO e Israel. El software de reconocimiento facial usado fue desarrollado por la compañía tecnológica israelí AnyVision, que había recibido inversiones significativas de Microsoft. En octubre de 2019, Microsoft contrató⁴² al ex fiscal general de EE. UU. Eric Holder para examinar cómo se estaba usando la tecnología de AnyVision y establecer si la empresa cumplía con los

principios éticos de Microsoft⁴³ sobre cómo debería usarse la tecnología de vigilancia biométrica. Esto sucedió al conocerse que AnyVision estaba llevando a cabo vigilancia masiva en Cisjordania/TPO.

En marzo de 2020, Microsoft retiró su apoyo financiero a AnyVision, a pesar de que anunciaron conjuntamente que la auditoría del Sr. Holder no confirmaba⁴⁴ ninguna infracción de los principios de Microsoft. La auditoría también encontró⁴⁵ que la tecnología de AnyVision “no ha sustentado ni sustenta programa alguno de vigilancia masiva en Cisjordania/TPO como reportaron algunos medios”. También existe la preocupación de que las Fuerzas de Defensa de Israel (IDF, por sus siglas en inglés) o la policía estén usando SRF en vivo para rastrear los movimientos de palestines en Cisjordania/TPO, como se mostró en un video de demostración de AnyVision⁴⁶ obtenido por NBC.

Vulneraciones de derechos y libertades

Los derechos a la privacidad, de reunión, de asociación y a la libertad de movimiento se ven comprometidos por este sistema de identificación biométrico que les palestines que buscan ingresar a Israel para trabajar no parecen tener forma de evitar. Este sistema también se presta a la creación de bases de datos policiales visuales para su uso futuro que podrían llevar a potenciales identificaciones erradas, arrestos y detenciones ilegítimas.

Acciones legales y de incidencia

La ACRI presentó una petición⁴⁷ al tribunal administrativo en Jerusalén en septiembre de 2020 luego de que las IDF se negaran a contestar una solicitud de acceso a la información sobre el uso de SRF en Cisjordania/TPO. Las IDF alegaron que la entrega de esta información revelaría las prácticas operativas y pondría en riesgo la seguridad nacional. Una petición adicional fue presentada por ACRI contra la policía de Israel, que también se negó a revelar cualquier información sobre su uso de SRF.

Temores de un apartheid basado en inteligencia artificial en Sudáfrica

Edwin Makwati, Legal Resources Centre

Qué

El despliegue en curso de 15.000 cámaras de circuito cerrado de videovigilancia (CCTV) que usan inteligencia artificial en Johannesburgo, Sudáfrica, ha suscitado temores de que, en ausencia de una correcta regulación, provocará un apartheid basado en inteligencia artificial⁴⁸, discriminación, amenazas a la seguridad y violaciones a la privacidad. Se teme que, a medida que más áreas instalen las cámaras Vumacam, que presentan sesgos intrínsecos contra personas no blancas y mujeres, esa implementación dé pie al perfilamiento racial y a la normalización de la vigilancia masiva.

DÓNDE JOHANNESBURGO, SUDÁFRICA

CUÁNDO DESDE 2019

Detalles adicionales

Vumacam es una empresa privada. La red de cámaras es financiada de manera privada, y las empresas de seguridad autorizadas pagan para acceder a la transmisión en sus áreas. Cámaras panorámicas y lectoras de patentes transmiten imágenes a través de una red de fibra óptica a un centro de datos que registra o busca en bases de datos de vehículos sospechosos, como aquellos que pueden haber sido robados. Los sistemas de aprendizaje automático realizan análisis de los videos para reconocer parámetros como objetos o comportamientos. Con suficientes cámaras, las computadoras podrían “vigilar” un barrio y notificar a fuerzas de seguridad privada en tiempo real cuando el algoritmo detecte algo que considere sospechoso. Las empresas de seguridad tienen un acuerdo contractual con Vumacam que les da acceso a la transmisión. En el caso de que necesiten grabaciones, tienen que solicitarlo a Vumacam con documentación oficial del Servicio de Policía de Sudáfrica (SAPS, por sus siglas en inglés).

Vulneraciones de derechos y libertades

Vumacam ha desmentido de forma categórica que sus cámaras usen tecnologías de reconocimiento facial⁴⁹.



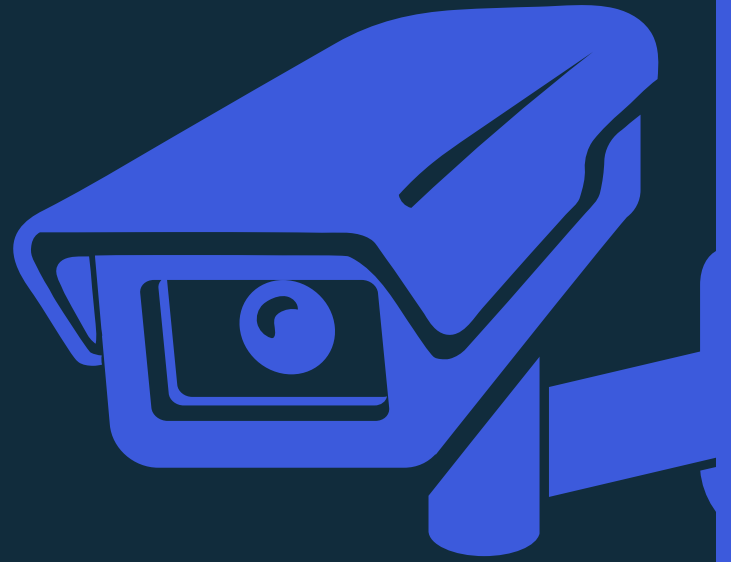
La constitución de Sudáfrica está basada en los valores de la dignidad humana, el logro de la igualdad y las libertades, y reconoce las desigualdades causadas por el pasado represivo del país. La instalación de SRF sin las garantías adecuadas es una amenaza a esos valores compartidos, puesto que estas vulneraciones irrestrictas desconocen la privacidad y libertad de expresión.

• EDWIN MAKWATI, ABOGADO E INVESTIGADOR LEGAL EN EL LEGAL RESOURCES CENTRE

De todos modos, estas cámaras comprometen el derecho fundamental a la privacidad, la noción del consentimiento tácito y la ciberseguridad y suponen un riesgo potencial de hackeo cuando la información almacenada puede ser filtrada, alterada o robada si no se protege suficientemente. Más importante aún, en un país con alta desigualdad racial, hay preocupaciones de que el sistema Vumacam refuerce esa desigualdad al identificar erróneamente a las personas no blancas.

Acciones legales y de incidencia

Diversas organizaciones sudafricanas de derechos y libertades civiles se han opuesto al proyecto Vumacam y afirman que no cumple con la Ley de Protección de Información Personal de Sudáfrica (POPIA, por sus siglas en inglés), una ley que busca proteger a las personas a través de la protección de su información personal con el fin de mitigar las consecuencias imprevistas de las tecnologías emergentes. Los grupos afirman que, de acuerdo con POPIA, Vumacam necesita el consentimiento de las personas para recolectar información personal como números de patentes. Sin embargo, Vumacam dice cumplir con la legislación. El LRC ha iniciado acciones legales contra el gobierno y proveedores de servicios de telefonía móvil en torno a la vigilancia general e impugnó la legislación sobre vigilancia.



Los SRF y

El derecho a la libertad de reunión y asociación

03

Los SRF y el derecho a la libertad de reunión y asociación

Ádám Rempert, Hungarian Civil Liberties Union (HCLU)

Las nuevas tecnologías pueden ser poderosas herramientas para facilitar manifestaciones, como protestas, sentadas y huelgas, porque permiten a los participantes organizar sus reuniones de manera más eficiente. Sin embargo, algunas pueden suponer nuevas amenazas a derechos fundamentales. Resulta especialmente preocupante que los SRF permiten a los gobiernos identificar, rastrear y crear bases de datos de ciudadanos que participan en manifestaciones pacíficas, prácticas que pueden inhibir o directamente suprimir la disidencia. Las organizaciones que componen INCLO han tomado acción legal en varios países para proteger los derechos de la gente a la libertad de reunión y asociación.

El derecho a reunirse pacíficamente y a la libertad de asociación está consagrado en varios tratados y convenciones internacionales fundamentales, incluyendo la Declaración Universal de los Derechos Humanos y el Convenio Europeo de Derechos Humanos. Este derecho es pilar fundamental de cualquier sistema democrático. No obstante, los SRF vulneran directamente este derecho al facilitar un tipo de vigilancia que, de por sí, puede servir para disuadir a las personas de participar en manifestaciones pacíficas. El riesgo que representan los SRF a la libertad de reunión y asamblea está aceptado universalmente, por lo que varias organizaciones internacionales, entre ellas, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos y la Agencia de los Derechos Fundamentales de la Unión Europea, promueven la adopción de salvaguardas en las legislaciones nacionales.

Las organizaciones que componen INCLO lideraron diversas acciones contra el uso ilícito de SRF. En julio de 2020, Agora International Human Rights Group, organización rusa miembro de INCLO, presentó una demanda ante el Tribunal Europeo de Derechos Humanos sobre el uso de reconocimiento facial contra manifestantes en Moscú. Fue la primera denuncia sobre el uso de sistemas de reconocimiento facial que recibió

dicho tribunal. Agora está representando a una activista y a un político por vulneración de su derecho a la reunión pacífica por la recolección de sus datos biométricos en momentos previos a una manifestación política. Les representados por Agora, así como por lo menos 20.000 otros participantes, solo pudieron acceder al lugar de la concentración pasando por detectores de metales equipados con cámaras de CCTV con uso de reconocimiento facial a la altura de los ojos.

En otro caso pionero relacionado con el uso de sistemas de reconocimiento facial por la policía en Gales del Sur, la organización de INCLO basada en el Reino Unido Liberty participó en una demanda que resultó en la declaración por un tribunal, en agosto de 2020, de que el uso de SRF por parte de la policía había violado el derecho a la privacidad bajo el CEDH⁵⁰, la primera decisión de este tipo en el Reino Unido. Después del fallo, Liberty reclamó que la policía cesara totalmente el uso de estos sistemas.

Mientras tanto, Dejusticia, en Colombia, solicitó información a la Fiscalía General de la Nación con relación a un helicóptero equipado con cámaras de reconocimiento facial que fue usado para monitorear determinadas manifestaciones. Lejos de negar la existencia de la tecnología, la policía previamente había hecho alarde de que el helicóptero podía identificar individuos a una distancia de 15 kilómetros y que era capaz de reconocer caras tapadas, afirmaciones que tendrían un obvio efecto disuasivo sobre manifestantes que desearan participar en las protestas. Sin embargo, la Fiscalía no pudo decirle a Dejusticia cuántas investigaciones criminales fueron abiertas a partir de la información reunida por las cámaras del helicóptero ni tampoco brindó una posición legal sobre el uso de reconocimiento facial.

INCLO y sus miembros siguen monitoreando todos los aspectos del uso de tecnología de reconocimiento facial, con un énfasis especial en la libertad de reunión y asociación.

Manifestantes bajo vigilancia en Moscú

Damir Gainutdinov, Agora

Qué

El uso indiscriminado de SRF durante una manifestación contra el gobierno en Moscú llevó a la recolección de datos biométricos de miles de personas opositoras, incluyendo a la activista Alena Popova y al político Vladimir Milov. Las personas que participaron de la manifestación tuvieron poca o ninguna elección sobre la recolección de sus datos, al tener que pasar por detectores de metales equipados con cámaras de CCTV instaladas a la altura de los ojos.

DÓNDE MOSCÚ, RUSIA

CUÁNDO 29 DE SEPTIEMBRE DE 2019

Detalles adicionales

Al menos 20.000 personas⁵², entre ellas, la activista Alena Popova y el político Vladimir Milov, participaron en una manifestación autorizada en Moscú en solidaridad con las personas arrestadas e imputadas⁵³ por participar en protestas pacíficas en respuesta a la exclusión de candidatas independientes de las elecciones legislativas de la ciudad de Moscú. En años recientes, Rusia ha emergido como una de las principales potencias en el desarrollo de SRF; el Gobierno defiende la expansión de su infraestructura de reconocimiento facial como medio para luchar contra el crimen y mantener el orden. Pero muchos activistas de derechos afirman que también ha sido utilizada para identificar a personas que participan en protestas y reprimirlas. A lo largo de 2019, se instaló una red de más de 105.000 cámaras por toda Moscú. El sistema fue usado para asegurar que las personas estuvieran cumpliendo las reglas de la cuarentena por el COVID-19, pero hoy continúa usándose para identificar a individuos en manifestaciones y protestas.

Vulneraciones de derechos y libertades

Agora International Human Rights Group, también conocido como Agora, sostiene que la recolección



El Estado no debería poder seguir cada paso que damos. El reconocimiento facial es uno de los primeros pasos hacia la creación de una dictadura digital. El Estado está obligado a proteger nuestra privacidad, pero, en su lugar, nos priva de ese derecho... Los sistemas de reconocimiento facial no tienen ningún lugar en nuestras calles.

• ALENA POPOVA, ACTIVISTA

de los datos biométricos de los manifestantes no tiene fundamento jurídico y vulnera el derecho a la privacidad y la libertad de reunión. Igualmente apunta a que el uso de sistemas de reconocimiento facial en protestas y manifestaciones por parte de las autoridades contribuye a la discriminación por motivos políticos.

Acciones legales y de incidencia

En enero de 2020, la Sra. Popova y el Sr. Milov presentaron una denuncia contra el gobierno de Moscú⁵⁴ en relación con el uso de SRF. En marzo, un tribunal la desestimó⁵⁵ argumentando que el uso de la tecnología por parte del gobierno era legal. En julio de 2020, presentaron otra denuncia frente al Tribunal Europeo de Derechos Humanos (TEDH)⁵⁶ por el uso de SRF en Rusia durante manifestaciones. Agora les representa en el proceso ante el Tribunal.

Un método para disuadir a manifestantes en Colombia

Daniel Ospina Celis, Dejusticia

Qué

Cientos de personas fueron parte de protestas multitudinarias⁵⁷ el 21 de noviembre de 2019 para expresar, entre otras cosas, su descontento con la labor del presidente Iván Duque. Por su magnitud, importancia y consecuencias para la seguridad, a estas protestas se les conoce como “21N”. Las protestas duraron casi dos semanas y hubo otras manifestaciones en enero, febrero y noviembre de 2020. Un día antes del inicio de las protestas del 21N, salió a la luz que un helicóptero equipado con tecnología de reconocimiento facial sobrevolaría Bogotá durante las manifestaciones⁵⁸. Según las autoridades, el propósito de este despliegue era identificar a los manifestantes que instigaran a la violencia. Sin embargo, en Dejusticia, consideramos que dicha comunicación fue un intento de las autoridades de disuadir a las personas de salir a protestar.

DÓNDE BOGOTÁ, COLOMBIA

CUÁNDO NOVIEMBRE DE 2019

“

El discurso público en Colombia apoya fuertemente la implementación de tecnología de reconocimiento facial en casi todos los aspectos de la vida (incluyendo multas de tránsito). El discurso general en torno del reconocimiento facial carece de análisis sobre el impacto que tiene sobre los derechos humanos y especialmente el derecho a la privacidad.

- DANIEL OSPINA CELIS, INVESTIGADOR SOBRE PRIVACIDAD, DEJUSTICIA

Detalles adicionales

Según la Policía Metropolitana de Bogotá, el helicóptero equipado con tecnología de reconocimiento facial se usa desde hace más de 3 años. En ese sentido, ¿por qué la policía y los medios decidieron informar (o recordar) que se usaría el helicóptero justo un día antes de las protestas masivas? Aparentemente las cámaras

de reconocimiento facial con las que cuenta el helicóptero son capaces de detectar rasgos faciales a una distancia de 15 kilómetros. La policía incluso afirmó que la tecnología era capaz de identificar los rostros que estuvieran cubiertos⁵⁹. A pesar de estas “bondades”, no hay evidencia de que alguna persona haya sido judicializada como resultado del uso efectivo de esta herramienta.

Vulneraciones de derechos y libertades

Este tipo de acciones tienen la potencialidad de disuadir a cualquier manifestante de salir a protestar. No en vano la comunicación se hace precisamente un día antes del 21N. Se trata de una acción que amenaza el derecho a la privacidad, la libertad de expresión y el derecho a la manifestación y reunión pacífica.

Acciones legales y de incidencia

Dejusticia le preguntó a la Fiscalía General de la Nación cuántas investigaciones criminales se habían abierto a partir de la información recolectada por los sobrevuelos de este helicóptero. La Fiscalía dijo que no contaba con la información solicitada. Dejusticia también preguntó por el fundamento legal y constitucional del procesamiento de imágenes por SRF. En su respuesta a la solicitud de acceso a la información de Dejusticia, la Fiscalía General de la Nación indicó que no podía dar un concepto legal sobre el reconocimiento facial porque esto podría afectar la imparcialidad judicial. La policía tampoco ha confirmado si se han llevado a cabo evaluaciones sobre el uso de SRF, específicamente para determinar el posible impacto de estos sistemas en los derechos fundamentales de los ciudadanos. Dejusticia sigue monitoreando este tema apremiante.



Los SRF y

El derecho a la privacidad

04

Los SRF y el derecho a la privacidad

Brenda McPhail, Canadian Civil Liberties Association

La tecnología de vigilancia facial tiene el potencial de convertir el derecho a la privacidad, reconocido a nivel internacional, en algo meramente ilusorio.

Si bien es cierto que existe una justificada preocupación general sobre el impacto discriminatorio por causa de la conocida incapacidad de muchos programas de reconocimiento facial para identificar correctamente caras que no sean blancas y masculinas, múltiples defensores de la privacidad advierten que, si estas tecnologías se vuelven lo suficientemente precisas como para reconocer individuos con piel de color serán aún más peligrosas.

Un sistema de reconocimiento facial lo suficientemente preciso puede volver imposible moverse por espacios públicos siendo tan solo una cara en la multitud. Los individuos identificados por defecto, sin posibilidad de anonimidad, no solo pierden la privacidad; sino que todos los derechos asociados se verán debilitados si el reconocimiento facial logra una aceptación generalizada.

La posibilidad de que las personas se sientan cómodas ejerciendo la libertad de asociación, el derecho al disenso y la libertad de expresión a menudo depende del hecho de no ser vigiladas. También es importante recordar que la privacidad no es solo un derecho individual sino un bien público. La igualdad de derechos, por ejemplo, se ve más fácilmente erosionada cuando los análisis faciales permiten la clasificación social.

Diferentes formas de vigilancia facial crean diferentes carencias o problemas de privacidad, como se desprende de la lectura de los estudios de caso nacionales de este informe. De igual manera, hay distintos niveles de riesgo para derechos individuales y colectivos dependiendo de si la tecnología es usada por el sector privado o por actores estatales, aunque las fronteras entre ambos son cada vez más difusas a medida que los estados se valen de productos del sector privado y los

vendedores compiten simultáneamente por contratos gubernamentales y ventajas comerciales.

Muchos miembros de INCLO han resaltado las severas violaciones a derechos que ocurren cuando las fuerzas de seguridad usan vigilancia facial. Ya sea con cámaras en espacios públicos (como se describe en el caso de la exitosa impugnación legal de Liberty al uso de SRF por la policía de Gales del Sur) o como resultado de la automatización del proceso de búsqueda de correspondencias entre imágenes de escenas de un crimen y fotos en posesión de la policía o a las cuales esta tiene acceso (como en la historia de identificación errónea de la ACLU), las consecuencias para los individuos atrapados en la red de vigilancia pueden ser graves.

A pesar de los riesgos potenciales, son pocas las jurisdicciones que, a través de los instrumentos legales existentes, protegen la privacidad de manera adecuada, y menos aún las que implementaron regulaciones específicas para esta tecnología invasiva. La tendencia a desplegarla en secreto, sin transparencia ni rendición de cuentas, exacerba aún más las preocupaciones sobre la privacidad, como muestra la Canadian Civil Liberties Association (CCLA) en su caso, en el que se describe el uso tras bambalinas de tecnología de Clearview AI por parte de fuerzas policiales en el país, sin el escrutinio de ninguna instancia reguladora que hubiera podido identificar que las imágenes en la base de datos de Clearview probablemente serían consideradas como obtenidas de forma ilegal bajo la ley canadiense.

La privacidad es un derecho humano y es una primera línea de defensa para muchos otros derechos. El impacto de las tecnologías de vigilancia facial sobre los derechos de las personas y los grupos de moverse por espacios públicos sin escrutinio estatal indebido amenaza con erosionar las libertades civiles y los derechos humanos de una manera incompatible con las libertades y valores democráticos.

Uso encubierto por parte de la policía en Canadá

Brenda McPhail, Canadian Civil Liberties Association

Qué

El uso encubierto de SRF revelado en Canadá da cuenta de preocupaciones sobre el posible uso más extendido de estos sistemas en el país. En 2020, fuerzas policiales en distintos lugares de Canadá admitieron⁶⁰ a regañadientes que habían estado probando el controversial SRF de Clearview AI, a pesar de que muchas de ellas lo habían desmentido inicialmente⁶¹. En mayo de 2019⁶², trascendió que la policía de Toronto había estado usando durante más de un año SRF para comparar imágenes de potenciales sospechosos tomadas en cámaras públicas o privadas con su base de datos interna de 1,5 millones de fotos policiales⁶³. Hasta 2017, el público tampoco sabía que la compañía Cadillac Fairview estaba usando SRF en centros comerciales en Calgary (y probablemente otros lugares también) para monitorear el tráfico de clientes, así como sus edades y géneros, una práctica ya suspendida⁶⁴.

DÓNDE EN UN NÚMERO DESCONOCIDO DE MUNICIPALIDADES EN CANADÁ, QUE INCLUYEN TORONTO Y CALGARY.

CUÁNDO 2019-2020

Detalles adicionales

La tecnología de reconocimiento facial de Clearview AI estaba siendo usada por la Policía Real Montada de Canadá y otras fuerzas regionales o municipales de distintas partes del país, sin divulgación pública, y, en muchos casos, aparentemente por iniciativa de individuos dentro de una fuerza sin autorización de sus superiores. La indignación pública y una investigación sobre dicha tecnología del Comisionado de Privacidad de Canadá contribuyeron a que Clearview AI retirara sus servicios del país. Esa investigación continúa y se anticipa que la manera en que Clearview obtenía imágenes para su base de datos, haciendo “scraping” de fotos sin consentimiento en redes sociales y otros sitios de internet, será declarada una violación de las leyes de privacidad canadienses. Cientos de miles, si no millones, de canadienses pueden haber sido incluidos en la base de datos. Muchas fuerzas solo admitieron haber usado la tecnología después de que



La tecnología de reconocimiento facial es demasiado poderosa y demasiado imperfecta para ser usada antes de que la sociedad haya tenido las conversaciones necesarias y nos hayamos preguntado si esta tecnología podrá alguna vez usarse sin socavar nuestras libertades fundamentales.

• BRENDA MCPHAIL, DIRECTORA DEL PROYECTO SOBRE PRIVACIDAD, TECNOLOGÍA Y VIGILANCIA, CCLA⁶⁵

investigaciones mediáticas y una filtración de datos⁶⁶ salieran a la luz.

Vulneraciones de derechos y libertades

Los SRF –y más aún cuando se usan de manera encubierta– tienen el potencial para eliminar nuestra posibilidad de ser una cara anónima en la multitud. Actores públicos y privados parecen tener sus propias y, con frecuencia, controversiales interpretaciones de las leyes de privacidad o explotan lagunas en la envejecida regulación canadiense sobre privacidad. La obtención de un consentimiento válido es ilusoria o, más frecuentemente, imposible. La discriminación, la identificación errónea, la obstrucción del debido proceso, el arresto y la detención indebida pueden ocurrir; sin embargo, hay pocas posibilidades de control público sobre tales perjuicios.

Acciones legales y de incidencia

La CCLA ha iniciado una serie de solicitudes de acceso a la información sobre los usos de los productos de Clearview, la cantidad de casos en que se usó durante investigaciones, el número de acusados identificados y la relación entre el uso de la tecnología y los cargos presentados. La organización está analizando cómo el programa de SRT de la policía de Toronto afecta los procesos legales contra personas identificadas con esta tecnología. La CCLA ha reclamado una moratoria sobre el uso de SRF mientras esté pendiente el debate público y la mejora de la regulación y participó en un estudio sobre reconocimiento facial conducido por la Oficina del Comisionado de Privacidad de Canadá.

Arrestada por una orden judicial inválida en Argentina

Margarita Trovato, Centro de Estudios Legales y Sociales

Qué

Una mujer identificada por una cámara con reconocimiento facial en la Ciudad de Buenos Aires fue interceptada por efectivos de la policía y detenida casi 15 años después de que se le emitiera una orden judicial de arresto. La orden había sido emitida en 2006 porque la mujer incumplió una obligación de presentarse a declarar como testigo en un juicio, a causa de que no había sido debidamente notificada. Para cuando fue detenida en 2019, la orden de detención que ella desconocía ya había vencido, de modo que su arresto fue ilegal.

DÓNDE BUENOS AIRES, ARGENTINA

CUÁNDO FROM APRIL 2019

“

In the city of Buenos Aires, mass facial recognition did not pass through the legislature or involve any type of political discussion. The software, how it was acquired, who implements it or under Qué regulations or control mechanisms are not known.

• INFORME ANUAL DEL CELS 2019 ⁶⁷

Detalles adicionales

Las autoridades de la Ciudad de Buenos Aires empezaron a usar reconocimiento facial en unas 10.000 cámaras⁶⁸ en la ciudad en abril de 2019 con la meta de detectar personas contra quienes se hubiera emitido una orden judicial de arresto⁶⁹. Sin embargo, el uso de cámaras con esta tecnología en el subterráneo de la ciudad ha llevado a detenciones de personas inocentes que fueron demoradas durante horas antes de ser liberadas. A pesar de reclamos de la sociedad civil, la Ciudad de Buenos Aires en octubre de 2020 adoptó un marco regulatorio y legal sobre reconocimiento facial excesivamente superficial, después de un debate abreviado que careció de un análisis pertinente sobre el impacto de la tecnología sobre los derechos humanos. Al día de la fecha, sigue sin saberse qué software se usa, cómo fue adquirido y quién lo implementa.

Vulneraciones de derechos y libertades

Una base de imágenes policial desactualizada y falsos positivos han llevado a arrestos ilegítimos, que han proyectado sospecha sobre personas inocentes y las han puesto en la ingrata posición de tener que demostrar su inocencia. Los principios del debido proceso y la equidad procesal se ven amenazados, mientras que la ausencia de discusión política sobre el uso y despliegue de esta tecnología va en contra de los principios democráticos. Los derechos a la privacidad, a la protección de la información personal y de los ciudadanos a conocer qué información ha sido compilada sobre ellos también se ven implicados.

Acciones legales y de incidencia

El CELS asistió a la mujer arrestada en Buenos Aires luego de su detención. También ha estado haciendo incidencia sobre que no solo hay problemas de violación a la privacidad con las cámaras de reconocimiento facial, sino que también hay un problema de precisión. Parece claro que la información suministrada al sistema no ha sido actualizada y que ninguna autoridad judicial o policial parece estar fijándose quién está siendo detectado y detenido ni por qué razón.

Cámaras Hikvision en un hospital infantil en Irlanda

Olga Cronin, Irish Council for Civil Liberties

Qué

Es posible que en el nuevo hospital nacional infantil en Irlanda se utilicen cámaras de CCTV Hikvision equipadas con sistemas integrales de reconocimiento facial como parte del sistema de seguridad. Estas cámaras, vinculadas con abusos de derechos humanos en China, pueden mapear rasgos faciales en imágenes capturadas y compararlas con una base de datos de imágenes distinta para confirmar la identidad de una persona.

DÓNDE HOSPITAL NACIONAL DE NIÑES, DUBLÍN, IRLANDA

CUÁNDO SE ESPERA QUE EL HOSPITAL SE ABRA EN EL 2022

Detalles adicionales

Hikvision ha sido ampliamente condenada porque su tecnología es utilizada para monitorear minorías musulmanas en China⁷⁰. La empresa de vigilancia recibió fuertes críticas por supuestamente proveer equipamiento en Xinjiang, donde uigures musulmanes están siendo víctimas de reclusión forzada en centros de detención⁷¹. En Estados Unidos, una ley prohíbe desde agosto de 2019 que las entidades federales de gobierno compren cámaras Hikvision⁷². La revelación de que el nuevo hospital infantil de Irlanda podría usar cámaras de reconocimiento facial de Hikvision fue publicada por primera vez en diciembre de 2019⁷³. Tras ello, el ministro de salud irlandés dijo al parlamento que “menos del 3% de las cámaras procuradas para el nuevo hospital infantil tienen la capacidad de realizar reconocimiento facial en alta definición”⁷⁴. Mientras tanto, el gobierno de la ciudad de Dublín ha dado marcha atrás⁷⁵ a sus planes de usar estas cámaras en centros comunitarios.

Una vocal del Departamento de Salud le dijo al ICCL que se llevaría a cabo una evaluación de todos los aspectos de los sistemas de seguridad a ser instalados en el hospital. También dijo que se



To protect everyone’s rights, including children’s, the State should not install these face surveillance systems in hospitals in the first instance, and certainly not in cooperation with private surveillance companies with controversial rights track records.

• ELIZABETH FARRIES, ASSISTANT PROFESSOR, UNIVERSITY COLLEGE DUBLIN DIGITAL POLICY PROGRAMME

realizaría una evaluación de impacto en la protección de datos (DPIA, por sus siglas en inglés) y que el sistema elegido cumpliría con la ley irlandesa de protección de datos de 2018 y el Reglamento General de Protección de Datos (RGPD) de la UE.

Vulneraciones de derechos y libertades

El reconocimiento facial es caro, impreciso y discriminatorio. Dado que Irlanda está sujeta a las reglas del RGPD, el uso de SRF probablemente sea ilegal. El uso de estos sistemas sobre niños hospitalizados sería increíblemente invasivo. Los niños cuentan con especial protección de sus datos personales. Desplegar sistemas de reconocimiento facial de esta manera chocaría con esas protecciones.

Acciones legales y de incidencia

El ICCL ha hecho incidencia contra el uso de estas cámaras en el hospital⁷⁶, mientras que el comisionado irlandés para la protección de datos ha advertido al hospital⁷⁷ que si tiene intenciones de usar SRF debe realizar una DPIA, porque el procesamiento de datos podría involucrar nuevas tecnologías, datos de niños, datos de categoría especial, según define el artículo 9 del RGPD⁷⁸, y procesamiento a gran escala en un área públicamente accesible.

La discrecionalidad del servicio secreto en Hungría

Ádám Rempert, Hungarian Civil Liberties Union

Qué

En Hungría, el despliegue de reconocimiento facial es esporádico y a menudo es usado para identificar personas buscadas por la justicia o cuyo paradero se desconoce, aunque el alcance real del uso de estos sistemas es en gran parte desconocido. Hasta ahora, el marco legal existente sobre recolección y acceso a datos personales no tiene previsiones sobre reconocimiento facial. Un informe reciente revela que la principal institución estatal autorizada para recolectar y controlar información confidencial a través de sistemas de reconocimiento facial es el Servicio Especial para la Seguridad Nacional (servicio secreto).

DÓNDE HUNGRÍA

CUÁNDO 2018 - 2019

“

Esta tecnología es nueva en tanto que ni siquiera hemos establecido los términos legales en húngaro para describir todos los conceptos relacionados. A esta altura, el uso de SRF se realiza de manera discrecional por parte del servicio secreto, lo cual significa que su uso correcto depende del sentido común y las buenas intenciones de los agentes del servicio secreto.

- ÁDÁM REMPERT, OFICIAL LEGAL, PROYECTO SOBRE PRIVACIDAD, HUNGARIAN CIVIL LIBERTIES UNION

Detalles adicionales

Una consulta de la HCLU enviada a la Autoridad Nacional de Protección de Datos (ANPD) en 2019 sobre el uso de SRF por parte del gobierno provocó una investigación que reveló que el servicio secreto, autorizado para usar el software de reconocimiento facial, lleva a cabo el proceso de identificación a solicitud de distintas ramas del gobierno. También conocimos por el informe de la ANPD que, en 2018, el reconocimiento facial fue usado de forma esporádica en relativamente pocos casos (6.000

veces), que llevaron a 209 solicitudes policiales de identificación individual y cuatro arrestos. Otra autoridad que usa reconocimiento facial es la oficina nacional de migraciones, que compara imágenes con los retratos de personas buscadas en listas publicadas por la policía húngara y por Interpol, Europol y el FBI en sus foros públicos.

También merece atención el despliegue por parte del Ministerio del Interior de un sistema centralizado de datos de imágenes recolectadas continuamente desde varios lugares vía una red nacional de 35.000 cámaras de CCTV. Esta tecnología es instalada por las ciudades y por la policía en espacios públicos, incluyendo autopistas, bancos y transportes públicos, y ofrece la posibilidad de almacenar y vincular los datos recolectados entre sí y con datos de otras fuentes.

Vulneraciones de derechos y libertades

Preocupa que el marco legal existente sobre la recolección y el acceso a datos personales no hace referencia específica al reconocimiento facial y permite la interpretación más amplia posible sobre cómo manejar esos datos, y como tal no puede garantizar la protección del derecho a la privacidad. Además, la HCLU remarca la preocupación de que en cualquier momento dado podría estar usándose SRF con la red de cámaras de CCTV existente, lo que ampliaría aún más la amenaza a la privacidad.

Acciones legales y de incidencia

No se han tomado acciones legales aún. Aunque el uso de SRF parece esporádico y limitado, la HCLU enfatiza la necesidad de desarrollar un marco legal preciso con referencia específica al reconocimiento facial.

Un sistema que ve a través de las mascarillas de COVID-19 en India

Siddharth Seem, Human Rights Law Network

Qué

A principios de 2020, el gobierno central de India aprobó el despliegue de un sistema automatizado de reconocimiento facial (AFRS, por sus siglas en inglés) a lo largo y ancho del país a partir de 2021. El sistema supuestamente permitiría que se extrajeran datos biométricos faciales de videos y cámaras de CCTV, que podrían ser contrastados con imágenes de individuos cuyas fotos se encuentran en bases de datos del Buró Nacional de Archivos Criminales (NCRB, por sus siglas en inglés). Supuestamente será el sistema de reconocimiento facial más grande del mundo en ser gestionado por un gobierno. En septiembre de 2020, trascendió que el NCRB quiere un AFRS que pueda identificar a personas que tengan puesto un barbijo. Debido al COVID-19, 300 millones de personas en las ciudades y estados más grandes de India actualmente deben usar barbijo o arriesgarse ser encarceladas⁷⁹.

DÓNDE EL SISTEMA SERÁ USADO POR LA POLICÍA A LO LARGO Y ANCHO DE INDIA

CUÁNDO LA FECHA LÍMITE DE LICITACIÓN FUE EL 8 DE OCTUBRE DE 2020, DESPUÉS DE SER EXTENDIDA 12 VECES

Detalles adicionales

El NCRB lanzó una licitación para llamar a ofertas de proveedores para desarrollar el AFRS nacional donde se describía a la herramienta de vigilancia como una aplicación web centralizada que será la base para una “plataforma de consulta de imágenes faciales a nivel nacional”⁸⁰. El NCRB planea que la policía pueda acceder al sistema mediante teléfonos celulares, con hasta 2.500 usuarios en simultáneo. Tras ser consultado sobre la correspondencia parcial de caras por el uso de barbijo, el NCRB clarificó que los potenciales ofertantes perderían puntos en la licitación si sus sistemas no pueden reconocer caras cubiertas con barbijos⁸¹. Esto se mantuvo a pesar de que algunos estudios mostraron que algunas pruebas de algoritmos de reconocimiento facial



Los planes del NCRB violan todo principio legal que gobierna el derecho a la privacidad y la protección de los datos. La ausencia de una ley de protección de datos en India profundiza los riesgos a la privacidad de cualquier programa por el que fuerzas de seguridad puedan recolectar, usar y controlar datos de la manera que les plazca. Adicionalmente, los problemas de imprecisión de esta tecnología presentan una amenaza a las minorías religiosas y los grupos socialmente marginados en India, que ya son regularmente implicados en supuestos crímenes de manera errónea.

• SIDDHARTH SEEM, LAW OFFICER, THE HUMAN RIGHTS LAW NETWORK IN DELHI (HRLN)

sobre caras parcialmente cubiertas por tapabocas presentaron porcentajes de error de hasta el 50 por ciento⁸² en algunos casos. El NCRB también dijo que los sistemas de los potenciales ofertantes tendrían que generar “informes exhaustivos de autenticación biométrica” que incluyeran el rostro y las huellas digitales de la persona.

Vulneraciones de derechos y libertades

La creación de un sistema nacional automatizado de reconocimiento facial, sin leyes robustas de protección de datos, podría derivar en un sistema de vigilancia masiva para toda la población y en la discriminación, exclusión y graves violaciones de derechos humanos fundamentales. Se desconoce cómo serán recolectados y almacenados los datos en este sistema ni quién o qué lo supervisará para garantizar derechos fundamentales.

Acciones legales y de incidencia

Expertes en derechos digitales y en privacidad han planteado serias preocupaciones sobre estos planes. Si bien no ha habido acción legal formal aún, varios grupos han enviado solicitudes al gobierno para que retire su propuesta.

Planes frustrados para armar una “rueda de identificación perpetua” con SRF en Australia Kieran Pender, Human Rights Law Centre

Qué

En 2018, el gobierno australiano propuso la creación de un marco para obtener, usar y compartir imágenes faciales y otros datos biométricos. El esquema propuesto hubiera establecido una base de datos centralizada con imágenes de registros de conducir, a la que agencias federales, regionales y locales hubieran podido acceder para usar SRF. Esto hubiera servido como una “rueda de identificación perpetua”: millones de australianos inocentes hubieran estado sujetos a búsquedas indiscriminadas, potencialmente en tiempo real, sin transparencia y con protecciones mínimas.

DÓNDE AUSTRALIA

CUÁNDO MAYO DE 2018-OCTUBRE DE 2019

“

Las nuevas capacidades de búsqueda y vigilancia deben estar gobernadas por la ley, y las leyes existentes son insuficientes para garantizar esto. No obstante, hemos concluido que la ley propuesta es manifiesta y peligrosamente insuficiente para este propósito.

• PRESENTACIÓN DEL HUMAN RIGHTS LAW CENTRE A INDAGACIÓN PARLAMENTARIA, MAYO DE 2018⁸³

Detalles adicionales

En 2017, el gobierno federal de Australia estableció un acuerdo intergubernamental de “servicios de verificación de identidades” con los gobiernos estatales. De esta manera, los ocho gobiernos regionales acordaron compartir imágenes de los registros de conducir y otros datos biométricos con el gobierno federal, el cual establecería un “centro de interoperabilidad” a través del cual las agencias de todos los niveles de gobierno podrían acceder a datos biométricos. Las leyes presentadas ante el parlamento australiano en 2018 proveían el fundamento jurídico para el establecimiento del centro y la base de datos. Según las leyes propuestas, las agencias podían consultar las bases de datos sin orden judicial o de manera indiscriminada, en tiempo real o después de los

hechos, sin mecanismo para que un individuo cuyos datos fueran consultados sea informado (y por ende sin capacidad para controvertir la búsqueda). No se proveyó ninguna razón convincente para el esquema más allá del potencial de una mayor eficiencia en el cumplimiento de la ley y la administración de gobierno.

Vulneraciones de derechos y libertades

El esquema propuesto hubiera erosionado significativamente las garantías de privacidad de todos los australianos. Normalmente, la legislación de privacidad australiana requeriría que los individuos den consentimiento explícito, específico, voluntario e informado a la recolección, uso y divulgación de datos biométricos; este esquema no incluía estos requisitos. También presentaba una amenaza importante a las libertades de expresión, de asociación y reunión, ya que las leyes propuestas no contenían garantías para el ejercicio libre de estos derechos. También había graves preocupaciones sobre el potencial de que el esquema, de ser establecido, pesara desproporcionalmente sobre grupos marginalizados o vulnerables.

Acciones legales y de incidencia

El HRLC estuvo al frente de la resistencia contra las leyes propuestas. La organización realizó diversas y exhaustivas intervenciones en el contexto de la indagación realizada por el Comité Conjunto sobre Inteligencia y Seguridad (PJCIS, por sus siglas en inglés) del parlamento australiano. Al mismo tiempo, realizó una significativa campaña mediática y de incidencia en torno a las preocupaciones sobre las leyes propuestas, articulada con otros actores de la sociedad civil.

En octubre de 2019, el influyente PJCIS aceptó las intervenciones del HRLC y otros actores de la sociedad civil y recomendó que se volvieran a redactar las leyes sobre la base de que el régimen propuesto sea “construido en torno a la privacidad, la transparencia y sujeto a robustas garantías”⁸⁴. Las posiciones del HRLC fueron ampliamente recogidas en el informe final del PJCIS. A noviembre de 2021, todavía no se habían presentado las nuevas versiones de los proyectos de ley ante el parlamento.

SRF sin regulación a lo largo y ancho de Kenia

Martin Mavunjina, Kenya Human Rights Commission (KHRC)

Qué

En septiembre de 2018, el servicio nacional de policía lanzó un sistema de reconocimiento facial⁸⁵ que involucró la instalación de miles de cámaras, que también usan tecnología de reconocimiento de las placas de automóviles, a lo largo de todas las calles y autopistas principales como parte de su sistema integrado de mando y control (Integrated Command and Control System). El reconocimiento facial también se está usando en las fronteras de Kenia⁸⁶, y 1.800 cámaras con capacidades de reconocimiento facial fueron desplegadas por todo Nairobi y Mombasa en 2014, número que creció hasta 2.100 en 2019. Sin embargo, el uso desregulado de SRF por parte de las fuerzas de seguridad ha resultado en la vulneración del derecho a la privacidad y la libertad de expresión y el debilitamiento de la protección de derechos y libertades fundamentales.

DÓNDE NAIROBI Y MOMBASA Y LAS FRONTERAS DE KENIA

CUÁNDO DESDE 2014

Detalles adicionales

Las cámaras con capacidades de reconocimiento facial en Nairobi y Mombasa fueron desplegadas como parte de un sistema de vigilancia que involucra la transmisión en vivo a la sede central del Servicio Nacional de Policía. Este sistema ha llevado, según la policía, a la recuperación de más de 4.000 vehículos robados. No obstante, el incremento en las estadísticas del nivel de criminalidad contradice la idea de que el sistema ayuda a reducir el crimen. Según el Buró Nacional de Estadísticas de Kenia, 7.434 crímenes fueron reportados en 2017 en Nairobi frente a los 6.732 en 2014. La violación de una mujer a plena luz del día⁸⁷ en el centro de negocios de Nairobi en 2018 ha llevado a que muchos cuestionen la eficacia del sistema. Dudas adicionales surgieron en 2019, cuando trascendió⁸⁸ que las cámaras carecían de componentes básicos para contribuir a evitar un crimen y tenían una capacidad limitada de almacenamiento de datos.



El uso continuado de SRF por las fuerzas de seguridad en Kenia les dará libertad y discreción para desplegar una vigilancia masiva, suprimir voces disidentes, restringir la libertad de expresión y cometer diversas violaciones de derechos humanos como agresiones, represión de manifestaciones pacíficas o incluso ejecuciones extrajudiciales.

• MARTIN MAVUNJINA, ABOGADO CONSTITUCIONAL Y DE DERECHOS HUMANOS, KENYA HUMAN RIGHTS COMMISSION

Vulneraciones de derechos y libertades

El uso desregulado de SRF por parte de las fuerzas de seguridad en Kenia ha suscitado preocupaciones fundamentales particularmente en torno a la protección de datos y al derecho a la privacidad, bajo el artículo 31 de la Constitución de Kenia. También existen preocupaciones relacionadas con el debido proceso, ya que la policía no necesita ni autorización judicial ni consentimiento de ninguna individuo mientras lleva adelante la vigilancia. La ley de protección de datos de 2019⁸⁹ provee un marco robusto para el manejo y la protección de datos personales, pero el gobierno ha sido lento en su implementación. Estas cámaras han sido usadas para realizar vigilancia masiva a manifestantes pacíficos dentro de Nairobi y pueden explicar por qué durante o después de este tipo de manifestaciones, algunos defensores de derechos humanos han sido ilegalmente arrestados o detenidos por la policía⁹⁰.

Acciones legales y de incidencia

La KHRC sigue interpellando a actores estatales relevantes sobre las implicancias negativas de los SRF y las preocupaciones fundamentales de derechos humanos que surgen del continuado uso de estos, con el fin de asegurar que el gobierno implemente normas y políticas que desarrollen un marco regulatorio. La organización ya ha desafiado anteriormente las tecnologías de vigilancia desplegadas por el estado a través del litigio estratégico⁹¹.

Conclusión

Tal como ilustra nuestro informe, el uso indiscriminado de sistemas de reconocimiento facial por fuerzas de seguridad y otras agencias gubernamentales se está extendiendo alrededor del mundo. Los impactos y efectos perjudiciales de esta tecnología en la vida de las personas solo están comenzando a emerger. Pero ya podemos afirmar sin dudas que el despliegue mundial de esta herramienta de vigilancia masiva está promoviendo una peligrosa normalización de la vigilancia.

En la medida en que esta tecnología permita el seguimiento de personas en tiempo real y la identificación de quiénes somos, adónde vamos y con quiénes nos encontramos, amenaza con crear un mundo donde la gente es vigilada e identificada cuando se manifiesta, va a eventos religiosos, ve a un médico o simplemente vive su vida cotidiana.

La proliferación de esta tecnología discriminatoria y profundamente invasiva, frecuentemente con poco o ningún debate público, significa que no solo estamos en riesgo de perder toda privacidad en espacios públicos, sino que también pone en jaque nuestros derechos a la libertad de expresión, de protesta e igualdad.

En muchos países, el uso de reconocimiento facial se fundamenta en la insuficiente legislación. Sin marcos legales rigurosos que aseguren la transparencia, la rendición de cuentas y la seguridad en el uso de esta tecnología, esta puede ser objeto de usos indebidos o, peor aún, abusos.

La venta masiva de datos personales, sin consentimiento, pone en entredicho de manera urgente la necesidad y proporcionalidad de esta tecnología, que contribuye a las siempre crecientes bases de datos que recolectan nuestra información personal. Más preocupante aún, este método de vigilancia está en abierta contradicción con el principio legal de presunción de inocencia, un derecho humano integral bajo la Declaración Universal de los Derechos Humanos de la ONU⁹². Las personas inocentes no tienen ningún lugar en las bases de datos criminales⁹³.

Notas finales

1. [The Global Expansion of AI Surveillance](#) Carnegie Endowment for International Peace, Steven Feldstein, septiembre de 2019
2. [Half of All American Adults are in a Police Face Recognition Database, New Report Finds](#), Center on Privacy & Technology at Georgetown Law, octubre de 2016
3. FBI, [Facial Recognition Technology: Ensuring Transparency in Government Use](#), SDeclaración ante el Consejo de Supervisión y Reforma de la cámara baja, Washington D. C., junio de 2019
4. [Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification](#) Joy Buolamwini and Timnit Gebru, 2018
5. [81% of ‘suspects’ flagged by Met’s police facial recognition technology innocent, independent report says](#), Sky News, julio de 2019
6. [Delhi violence: Over 1900 faces recognised through facial recognition, says Amit Shah](#), The Economic Times, marzo de 2020
7. [China: facial recognition and state control](#), The Economist, octubre de 2018
8. [Statement on principles and prerequisites for the development, evaluation and use of unbiased facial recognition technologies](#), ACM Consejo de Política Tecnológica para EE. UU., junio de 2020
9. [Ed Bridges V South Wales Police](#), Tribunal de Apelaciones del Reino Unido, Bailii
10. [La compañía misteriosa que podría acabar con la seguridad que conocemos](#), New York Times, Kashmir Hill, enero de 2020
11. [Clearview AI ceases offering its facial recognition technology in Canada](#), Oficina del Comisionado canadiense para la Privacidad, julio de 2020
12. [Milov filed a lawsuit against the Moscow authorities and the Central Internal Affairs Directorate over face recognition technology](#), Kommersant, enero de 2020
13. [Police and Military Use of Facial Recognition Technology](#), ACRI, septiembre de 2020
14. [Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión](#), Asamblea General de la ONU, Consejo de Derechos Humanos, 41er período de sesiones, 24 de junio al 12 de julio de 2019
15. [Declaración Universal de los Derechos Humanos](#)
16. [Pacto Internacional de Derechos Civiles y Políticos](#)
17. [African Charter on Human and People’s Rights](#)
18. [Convenio Europeo de Derechos Humanos](#)
19. [Convención Americana sobre Derechos Humanos](#)
20. [ASEAN Human Rights Declaration](#)
21. [Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión](#), Asamblea General de la ONU, Consejo de Derechos Humanos, 41er período de sesiones, 24 de junio a 12 de julio de 2019
22. [One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority](#), New York Times, abril de 2019
23. [Ed Bridges v South Wales Police, UK Court of Appeal judgment](#)
24. [Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión](#), Asamblea General de la ONU, Consejo de Derechos Humanos, 41er período de sesiones, 24 de junio al 12 de julio de 2019
25. [Liberty wins ground-breaking victory against facial recognition tech](#), Liberty, agosto de 2020
26. [Ed Bridges V South Wales Police](#), Tribunal de Apelaciones del Reino Unido, Bailii

27. [Liberty wins ground-breaking victory against facial recognition tech](#), Liberty, agosto de 2020
28. [Petition: Resist facial recognition](#), Liberty
29. [Study finds gender and skin-type bias in commercial artificial-intelligence systems](#), MIT News, febrero de 2018
30. [Face Recognition Vendor Test \(FRVT\) Part 3: Demographic Effects](#), NIST, diciembre de 2019
31. [Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart](#), ACLU, junio de 2020
32. [Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time](#), Vice, junio de 2020
33. [Wrongfully Arrested Because of Flawed Face Recognition Technology](#), ACLU, junio de 2020
34. [Detroit police work to expunge record of man wrongfully accused with facial recognition](#), The Detroit News, junio de 2020
35. [ACLU of Michigan complaint re: use of facial recognition](#), ACLU, junio de 2020
36. [Community control over police surveillance](#), ACLU
37. [Tell the Detroit City Council: Say No to unchecked government surveillance](#), ACLU Michigan
38. [Despite pausing sales to police, company has not made same commitment for sales to federal law enforcement](#), ACLU, junio de 2020
39. [Gil-Gan Mor](#), ACRI, Twitter
40. [The Global State of Facial Recognition](#), Digital Information World, julio de 2020
41. [Face Recognition Lets Palestinians Cross Israeli Checkposts Fast, But Raises Concerns](#), NPR, agosto de 2019
42. [Microsoft hires Eric Holder to audit AnyVision over use of facial recognition on Palestinians](#), NBC, noviembre de 2019
43. [Facial recognition: It's time for action](#), Microsoft, diciembre de 2018
44. [Microsoft divests from Israeli facial-recognition startup](#), AP, marzo de 2020
45. [Findings of AnyVision Audit](#), Covington, marzo de 2020
46. [Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians?](#), NBC News, octubre de 2019
47. [Police and Military Use of Facial Recognition Technology](#), ACRI, septiembre de 2020
48. [Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa](#), Vice, noviembre de 2019
49. [Vumacam defends Joburg smart camera network](#), iWeb, diciembre de 2019
50. [Ed Bridges v South Wales Police](#), UK Court of Appeal judgment
51. [Activists appealed to the European Court of Human Rights for the use of technology of facial recognition at rallies](#), Rusbankrot, julio de 2020
52. [Thousands demand protesters freed in Moscow rally](#), BBC, septiembre de 2019
53. [The "Moscow Case": Qué You Need to Know](#), Human Rights Watch, octubre de 2019
54. [Milov filed a lawsuit against the Moscow authorities and the Central Internal Affairs Directorate over face recognition technology](#), Kommersant, enero de 2020
55. [The court dismissed the claim of Milov and Popova on the illegal use of face recognition technology in the Moscow video surveillance system](#), MBK, marzo de 2020
56. [Moscow's Use of Facial Recognition Technology Challenged](#), Human Rights Watch, julio de 2020
57. [Student Protester's Death Sparks Fresh Protests in Colombia. Here's Qué to Know](#), TIME, noviembre de 2019
58. [Así es el halcón, el helicóptero que vigilará el paro en Bogotá usando reconocimiento facial](#), Semana, noviembre de 2019

59. [Desde helicópteros, Policía haría reconocimiento facial a encapuchados](#), Publimetro, noviembre de 2019
60. [Police use of facial recognition program breaks ‘trust relationship’ with public, privacy expert says](#), CBC, febrero de 2020
61. [Facial recognition app Clearview AI has been used far more widely in Canada than previously known](#), York Region, febrero de 2020
62. [Privacy advocates sound warning on Toronto police use of facial recognition technology](#), CBC, mayo de 2019
63. [Toronto police have been using facial recognition technology for more than a year](#), The Star, mayo de 2019
64. [A quick win for privacy rights: CCLA VS Cadillac](#), Canadian Civil Liberties Association, octubre de 2018
65. [Can your face be your undoing: The perils of facial recognition](#), Centre For Free Expression, diciembre de 2019
66. [Clearview AI’s entire client list stolen in data breach](#), CNET, febrero de 2020
67. [El secreto: la seguridad nacional como coartada para un Estado sin controles](#), Derechos Humanos en la Argentina Informe 2019, CELS
68. Ibid
69. [Desde el 15 de abril buscarán a prófugos con sistema de reconocimiento facial](#), Ámbito, abril de 2019
70. [‘China: facial recognition and state control’](#), The Economist, octubre de 2018
71. [China steps up surveillance on Xinjiang Muslims](#), Financial Times, 18 de julio de 2018
72. [Life after the NDAA](#), Security Info Watch, agosto de 2019
73. [Ireland National Children’s Hospital Chooses Hikvision End-to-End With Facial Recognition](#), IPVM, diciembre de 2019
74. [National Children’s Hospital](#), Irish parliamentary debate, Oireachtas, diciembre de 2019
75. [DCC to cease using ‘blacklisted’ CCTV firm](#), Business Post, 17 de mayo de 2020
76. [Facial recognition technology](#), Irish Council for Civil Liberties
77. [Watchdog warning over mooted facial recognition cameras at Children’s Hospital](#), Irish Examiner, diciembre de 2019
78. Ver el artículo 9 del RGPD (Tratamiento de categorías especiales de datos personales) en <https://www.boe.es/doue/2016/119/L00001-00088.pdf>
79. [Coronavirus: India makes face masks mandatory for more than 300m people, punishable by up to six months in prison](#), Independent UK, abril de 2020
80. [Exclusive: Concerns around number of active users, and ‘backdoors’ raised at an NCRB facial recognition meeting](#), Medianama, julio de 2020
81. [India’s NCRB to test automated facial recognition system on ‘mask-wearing’ faces](#), Medianama, septiembre de 2020
82. [NIST Launches Studies into Masks’ Effect on Face Recognition Software](#), NIST, julio de 2020
83. [Human Rights Law Centre: The dangers of unregulated biometrics use: Submission to the Inquiry into the Identity-matching Services Bill 208 and the Australian Passports Amendment \(Identity-matching Services Bill\) 2018](#)
84. Identity-matching Services Bill 2019, [List of Recommendations from Australia’s Parliamentary Joint Committee on Intelligence and Security](#)
85. [Kenyan police launch facial recognition on urban CCTV network](#), Biometric Update, septiembre de 2018

86. [NEC facial recognition border tech for Kenya as airport biometrics rollouts continue](#), Biometric Update, octubre de 2019
87. [Police arrest street urchin who raped woman in broad daylight](#) Nairobi News, abril de 2018
88. [Interior Ministry on the spot over Sh15bn 'faulty' CCTV cameras](#) The Star, julio de 2019
89. [Data Protection Act](#)
90. [Police Arrest Many During #SabaSabaMarchForOurLives in Nairobi](#), Missing Voices, julio de 2020
91. [Petition 56, 58 & 59 of 2019](#) (Consolidated), Kenya Law
92. Artículo 11, [Declaración Universal de los Derechos Humanos, ONU](#)
93. [Half of All American Adults are in a Police Face Recognition Database, New Report Finds](#), Center on Privacy & Technology at Georgetown Law, octubre de 2016

Agradecimientos

INCLO quiere agradecer a Andreea Anca y Taryn McKay, la consultora de comunicación, y la diseñadora gráfica de INCLO, respectivamente, por su enorme contribución al concepto, contenido y arte de este informe.

Título original

In Focus. Facial Recognition Tech Stories and Rights Harms from Around the World

Acerca de INCLO



INCLO es una red de 15 organizaciones independientes y nacionales de derechos humanos alrededor del mundo. Trabajamos juntas para fortalecer la promoción de derechos y libertades fundamentales. Juntas somos Agora International Human Rights Group (Agora) en Rusia, la American Civil Liberties Union (ACLU), la Association for Civil Rights in Israel (ACRI), la Canadian Civil Liberties Association (CCLA), el Centro de Estudios Legales y Sociales (CELS) en Argentina, Dejusticia en Colombia, la Egyptian

Initiative for Personal Rights (EIPR), la Hungarian Civil Liberties Union (HCLU), el Human Rights Law Centre (HRLC) en Australia, la Human Rights Law Network (HRLN) en India, el Irish Council for Civil Liberties (ICCL), la Kenya Human Rights Commission (KHRC), la Commission for the Disappeared and Victims of Violence (KontraS) en Indonesia, el Legal Resources Centre (LRC) en Sudáfrica y Liberty en el Reino Unido.

Conozca más en inclo.net.