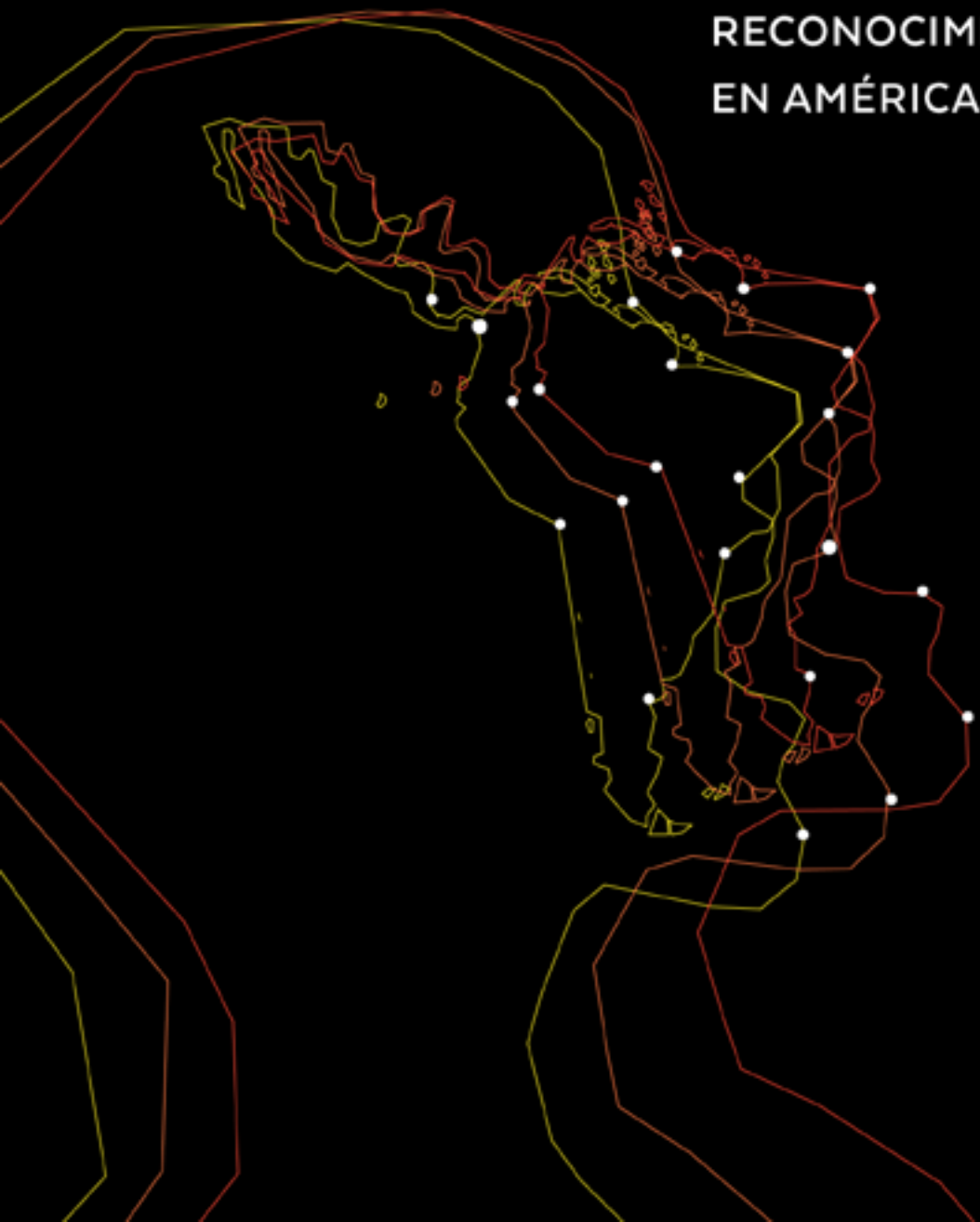
LATIN AMÉRICA
IN A GLIMPSE

CAPÍTULO 1

MAL DE OJO

RECONOCIMIENTO FACIAL EN AMÉRICA LATINA



DERECHOS DIGITALES
América Latina

DERECHOS DIGITALES
América Latina

Este informe fue realizado por Derechos Digitales y es un extracto de la edición 2019 de Latin America in a Glimpse, a publicarse en el mes de diciembre.

Texto por Vladimir Garay.

Diseño y diagramación por Constanza Figueroa.

Noviembre de 2019.

CAPÍTULO 1

MAL DE OJO

RECONOCIMIENTO FACIAL EN AMÉRICA LATINA

Por Vladimir Garay

"Me podrían haber arruinado la vida; a mí y a mi familia".[1] Esa es la reflexión que hace Guillermo Ibarrola frente a la cámara de A24, tras ser puesto en libertad después de estar seis días detenido por un crimen que no cometió, víctima de una pesadilla tecno-kafkiana.

Mientras se encontraba en Retiro, la principal terminal de omnibuses de Buenos Aires, dos policías se acercaron a Ibarrola y lo detuvieron. El sistema de reconocimiento facial que desde abril de 2019 opera en la capital argentina lo había identificado como responsable de un robo ocurrido en 2016 en Bahía Blanca.

Pero Ibarrola nunca había estado en Bahía Blanca ni tampoco había participado de ningún delito. El sistema había cometido una equivocación que solo fue enmendada seis días más tarde, mientras estaba siendo trasladado a una cárcel provincial. Mientras se encontraba detenido, Ibarrola intentó explicar que debía tratarse de un error. No importó, la máquina había dado ya un veredicto.

La implementación de sistemas de identificación biométrica - y particularmente de reconocimiento facial - ha sido uno de los puntos más debatidos durante los últimos años en la intersección entre tecnología y derechos fundamentales. Las promesas de exactitud, precisión y diligencia con las que se ha querido promocionar este tipo de tecnologías ha encontrado varias respuestas favorables entre los gobiernos y entidades estatales en América Latina, que suelen publicitar con gran pompa los esfuerzos realizados por incorporar estas técnicas a sus actividades, como símbolo de modernización.

Sin embargo, la experiencia internacional ha mostrado que las tecnologías de reconocimiento facial conllevan una serie de problemáticas difíciles de sortear y que las autoridades rara vez mencionan a la hora de anunciar públicamente la intención de poner en funcionamiento un sistema de este tipo. A la dificultad inherente a proteger debidamente datos altamente sensibles como los biométricos, se suma el alto porcentaje de falsos positivos arrojado por distintos sistemas de reconocimiento facial en funcionamiento alrededor del mundo, particularmente cuando se trata de personas de tez oscura, personas trans o no binarias.

En un experimento realizado por la American Civil Liberties Union (ACLU) el software de reconocimiento facial desarrollado por Amazon reconoció erróneamente a 28 congresistas estadounidenses como

1 Más información en https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien

autores de algún crimen, con un número desproporcionadamente alto de personas de color entre ellos.[2] El proyecto Gender Shades,[3] desarrollado por la investigadora Joy Buolamwini, demuestra que las tecnologías de reconocimiento facial disponibles en el mercado tienen grandes dificultades identificando mujeres de color, y obtienen sus mejores resultados cuando los sujetos analizados son hombres blancos.

Al mismo tiempo, la promesa de un sistema de reconocimiento facial completamente eficaz – imposible como es – no evoca precisamente un escenario idílico, sino más bien una distopía orwelliana, donde cada movimiento puede ser observado, registrado y escudriñado. Es por ello que, en una de sus editoriales, el periódico inglés The Guardian catalogó al reconocimiento facial como un peligro para la democracia[4] y cuatro ciudades estadounidenses – Oakland, San Francisco Berkley y Somerville, Massachusetts- la han prohibido.[5]

A todos los problemas anteriormente mencionados, en América Latina se suma un actuar muchas veces opaco y una interpretación antojadiza de leyes que no fueron concebidas para lidiar con las implicancias de este tipo de tecnologías, configurando un escenario de altas incertezas y muchas zonas grises, particularmente en relación con la defensa de los derechos fundamentales de las personas sometidas a estos sistemas. Estos problemas se agudizan cuando la tecnología es utilizada en tareas relativas a la persecución criminal y el orden público, donde la información muchas veces se vuelve inaccesible, escudada bajo leyes de seguridad nacional que le permiten funcionar sin control. Al respecto, los casos de Paraguay y Argentina son ilustradores.

En marzo de 2019, el Gobierno de la ciudad de Buenos Aires anunció la implementación de un sistema de reconocimiento facial para detectar prófugos y rebeldes de todo el país. Se trata de una nueva adhesión al sistema de biovigilancia pública de la ciudad, que ya contaba con una extensa red de cámaras, a algunas de las cuales se les ha adosado un software de reconocimiento facial, particularmente aquellas dispuestas en terminales y estaciones del tren subterráneo, el Subte.

"Sabemos que son alrededor de 200 cámaras que están usando ese software. El Gobierno no dice en qué estaciones están ni en qué cámaras están dentro de se subte. Desde ADC hicimos un pedido de acceso a la información para que nos informen eso y nos negaron esa información en base a razones de seguridad", explica Eduardo Ferreyra de la Asociación por los Derechos Civiles (ADC).

Algunas de las materias incluidas en el acceso a la información pública realizado por ADC dicen relación con la legalidad de la iniciativa y los protocolos de control que lo rigen, los aspectos técnicos del sistema y la composición de la base de datos utilizada. En opinión de la organización, las respuestas no fueron suficientemente precisas.[6]

El caso paraguayo es similar. Desde mediados del año pasado, el centro histórico de Asunción, el aeropuerto de la ciudad y las terminales de buses está siendo vigiladas por un sistema de reconocimiento facial donado por la Comisión Nacional de Telecomunicaciones (CONATEL) al Ministerio del Interior. "El ente regulador de comunicaciones tiene un fondo, que se llama Fondo Universale, que es exclusivamente para conectividad. Y, extrañamente, lo están utilizando para compras de seguridad y donando a otras instituciones del Estado, a través de convenios interinstitucionales", explica Maricarmen Sequera, directora ejecutiva de TEDIC.

Puesto que CONATEL no forma parte del convenio de contrataciones públicas, la licitación se realizó de

2 Más información en https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

3 Disponible en http://gendershades.org/

4 Disponible en https://www.theguardian.com/commentisfree/2019/jun/09/the-guardian-view-on-facial-recognition-a-danger-to-democracy

5 Más información en https://gizmodo.com/berkeley-becomes-fourth-u-s-city-to-ban-face-recogniti-1839087651

6 Toda la información sobre el requerimiento se puede revisar en https://adcdigital.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/

forma cerrada. Ante la total oscuridad con la que se estaba operando, TEDIC interpuso un recurso de acceso a la información pública con una serie de preguntas respecto al funcionamiento del sistema, incluyendo la geolocalización de las instalaciones, la base de datos utilizada y también respecto a la evaluación de impacto previa.

"La respuesta a esa solicitud de acceso fue parcial - advierte Sequera - Nos pasaron cierta información, pero era información que a la que ya habíamos accedido y no realmente sobre las preguntas que hicimos. Entonces apelamos y en la primera instancia el Ministerio del Interior dice que la otra información no la pueden dar por cuestiones de seguridad nacional".

Sin embargo, la ley paraguaya establece que para que una información sea reservada debe ser expresamente establecida por ley, no siendo este el caso. "Metieron este tema dentro de una mesa de seguridad nacional que tiene el Sistema de Inteligencia y con eso justificaron que todo lo que se discuta ahí es de seguridad nacional. Apelamos, y en la segunda instancia de nuevo los tres jueces aprobaron la posición del ministerio del interior, sin argumento",[7] declara Sequera.

Esta reticencia a transparentar información relativa al funcionamiento de los sistema de reconocimiento facial es preocupante, pues, como acota Leandro Ucciferri en un texto a propósito de la solicitud de transparencia realizado por ADC, "El reconocimiento facial, en particular cuando se lo usa con fines de investigación criminal, tiene el potencial de interferir directamente con derechos como la privacidad, la libertad de expresión, reunión y asociación, la no discriminación y garantías constitucionales como el debido proceso y la presunción de inocencia".

La falta de disposición para entregar información de cuestiones tan básicas como los proveedores de la tecnología que se está utilizando impide incluso hacerse una idea general respecto a la calidad de la herramienta en uso. Y es que no todos los sistemas de reconocimiento facial son iguales: las pruebas realizadas por la Metropolitan Police de Londres entre 2016 y 2018 arrojaron una taza de falsos positivos del 96%.[8] Si alguna iniciativa local considerara usar la misma tecnología sería importante saberlo.

En ese sentido, el caso boliviano es diferente. Presentado a fines de agosto y catalogado por el Ministro de Gobierno, Carlos Romero, como el programa de seguridad ciudadana más moderno de todo el continente,[9] Bol-110 es un ambicioso proyecto de adquisición de tecnologías de vigilancia "que van a estar en todo: en escuelas, taxis, hospitales", explica Hugo Miranda de Internet Bolivia.

Aquí, la tecnología está a cargo de la empresa estatal china CEIEC, responsable también de la infraestructura del programa ECU-911[10] en Ecuador. Coincidentemente, el financiamiento viene también por parte del Banco Nacional de China, Eximbak, que facilitó a Bolivia la suma de 105 millones de dólares para poner en marcha Bol-110.[11] Y aunque el proyecto no alcanzó a ser aprobado por el Poder Legislativo antes de la elección presidencial del 20 de octubre, los equipos ya fueron adquiridos.

"No es regular, no debería haber sucedido algo así, porque no tiene sentido comprar equipos que luego no se sabe cómo se van a utilizar. Pero como la voluntad estaba depositada sobre todo en el financiador, entonces pueden comenzar a hacer los procesos y luego darse cuenta de que necesitan un marco legal; me da la impresión de que eso es lo que ha sucedido. Probablemente incluso – estoy ahora especulando - había

7 Toda la información relativa a los requerimientos de acceso a información pública se encuentran en https://www.tedic.org/quien-vigila-al-vigilante-reconocimiento-facial-en-asuncion/

8 Más información en https://www.independent.co.uk/news/uk/home-news/facial-recognition-london-inaccurate-met-police-trials-a8898946.html

9 En https://www.youtube.com/watch?v=IAW3I8Dfngw

10 Más información en https://www.nytimes.com/es/2019/04/24/ecuador-vigilancia-seguridad-china/

11 Más información en https://m.eldiario.net/?n=65&a=2017&m=01&d=11

una necesidad de comprar en esta gestión esos equipos. Y, paralelamente, han ido proyectando la ley; y eso, como toma más tiempo, está saliendo retrasado", explica Eliana Quiroz de Internet Bolivia.

A pesar del incierto futuro político del país, Quiroz cree que el programa difícilmente será abandonado: es un proyecto hecho para la policía, que ha tenido un rol prominente en el proceso del nuevo gobierno transitorio.

Uno de los aspectos más llamativos sobre Bol-110 es que propone un ejercicio de coordinación mayúsculo de instituciones públicas y privadas relacionadas a la atención de urgencias, incidentes, emergencias y desastres, que incluye a la Policía, el sistema de salud, la Defensa Civil y Bomberos. Mediante un mandato de interoperabilidad, estas instituciones están obligadas a compartir información con el programa, por lo que su alcance se expande de manera bastante amplia a lo largo de todo el sistema social.

En ese sentido, Quiroz explica que Bolivia carece de una ley de protección de datos personales que restrinja el modo en que los datos puedan ser utilizados. "La policía depende del Ministerio de Gobierno y el Ministerio tiene, por mandato, la seguridad ciudadana. No hay -que yo sepa- ninguna restricción para utilización de esta tecnología y, me atrevería a decir, que tiene toda la posibilidad, la capacidad y el mandato de hacerlo. El problema es que no tiene el marco legal de protección de datos, porque eso no existe en Bolivia. Tenemos solamente articulado en la Constitución Política del Estado acerca de privacidad, que es muy genérico".

Esto no es del todo inusual. Aunque la mayoría de los países latinoamericanos en los cuales se ha implementado o existe un proyecto relativo al reconocimiento facial tienen leyes de protección a los datos personales, en la mayoría no existe una mención explícita a los datos biométricos ni su tratamiento, lo cual no necesariamente implica que carezcan de resguardo legal.

Para el caso argentino, Eduardo Ferreyra puntualiza: "La ley no establece expresamente ninguna disposición sobre datos biométricos, pero sí establece una disposición de datos sensibles, y nosotros de ADC creemos que claramente los datos biométricos entran en la definición de datos sensibles, que es información que revele cuestiones básicas de la identidad de una persona. Aparte, el derecho a la privacidad es derecho constitucional argentino y la Corte Suprema y distintos tribunales han dicho que tiene fuerte carácter expansivo, por lo cual, si bien expresamente no lo dice, está claro que pertenece a un dato sensible".

Una cuestión similar ocurre en Chile, donde los datos sensibles están sujetos al más alto estándar de protección que establece la ley y solamente pueden ser tratados cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares. Y aunque no cabe duda de que los datos biométricos califican como datos sensibles,[12] ello no impidió que una cadena de centros comerciales implementara un sistema de reconocimiento facial con fines de seguridad en uno de sus malls a fines de 2018[13] y que anunciara su expansión a otras de sus locaciones en 2019.[14]

La experiencia chilena es particular por una serie de razones. En primer lugar, porque en el caso del sistema de reconocimiento facial de Mall Plaza, se trata de una implementación privada sobre un espacio semi-público. En segundo lugar, porque el software utilizado por la cadena de centros comerciales fue testeado por la Policía de Investigaciones, arrojando una altísima taza de falsos positivos, que asciende al 90%.[15]

12 Para mayor información sobre esta interpretación en el caso chileno, ver La biometría en Chile y sus riesgos de Romina Garrido y Sebastián Becker https://revfono.uchile.cl/index.php/RCHDT/article/view/45825/48403

13 Más información en https://www.derechosdigitales.org/12623/sobre-la-ilegalidad-de-la-implementacion-de-un-sistema-de-reconocimiento-facial-en-mall-plaza/

14 Más información en https://www.cooperativa.cl/noticias/pais/policial/robos/mall-plaza-implementara-reconocimiento-facial-tras-violentos-asaltos/2019-09-04/081957.html

15 Más información en https://derechosdigitales.tumblr.com/post/183543851946/reconocimiento-facial-en-mall-plaza-90-de-falsos

Y en tercer lugar, porque el otro sistema de reconocimiento facial actualmente en funcionamiento no cumple funciones de seguridad, sino que busca vigilar la administración de un beneficio social. El sistema desplegado en la red de metro de la ciudad de Valparaíso busca controlar que los usuarios de tarjetas de tarifa reducida, estudiantes y personas de la tercera edad, no presten sus tarjetas a otras personas.[16] No hay información respecto a las pérdidas monetarias que esta práctica significa para la red de metro, ni tampoco del costo de la implementación del sistema de reconocimiento facial.

Una cuestión similar ocurre en Brasil. En São Paulo se implementó hace dos años el uso de cámaras de reconocimiento facial en el sistema de transporte público, con la justificación de que ayudarían a evitar el fraude en el uso de beneficios sociales asociados al transporte. En estos dos años el sistema ha bloqueado más de 300 mil tarjetas[17] supuestamente usadas indebidamente. Por otra parte, la municipalidad ha anunciado la suspensión total de las tarjetas anónimas y ha implementado medidas para obligar el registro de las tarjetas con datos de identificación únicos y residenciales. En una ciudad de las dimensiones de São Paulo, el bloqueo o imposibilidad de acceso a medios de transporte puede tener un gran impacto en la vida y el desarrollo de las personas, particularmente aquellas no registradas, como migrantes y las personas sin techo.

Mientras tanto, Argentina ha implementado un proyecto conocido como Sistema de Identidad Digital (SID), con el objetivo de simplificar y agilizar los trámites que realizan las personas con el Estado, permitiendo validar la identidad mediante el uso de reconocimiento facial.[18] Las imágenes son contrastadas con la base de datos del Registro Nacional de las Personas (RENAPER), que contiene las fotografías de todas las personas ciudadanas y residentes en Argentina.[19] ADC mira este desarrollo con bastante preocupación; como explica Eduardo Ferreyra "nos enteramos de casos de gente que no le funcionaba la identificación y no había otra alternativa para verificar identidad. La única respuesta era que prueben de nuevo". Ante problemas de este tipo, que potencialmente podrían dejara a personas fuera de los programas sociales, producto de fallas en los sistemas de identificación, es necesaria la habilitación de mecanismos alternativos.

Por su parte, en Ecuador avanza una iniciativa del Ministerio de Inclusión Económica y Social, que busca reemplazar el método de registro de poblaciones específicas que usan los servicios del ministerio, particularmente niños, niñas, adolescentes, personas de tercera edad y personas con discapacidades, en condición de pobreza extrema. Por medio de un acuerdo ministerial, el proyecto busca reemplazar el método actual de registro por uno de reconocimiento facial.

"No existe información que de cuenta de cuáles son las deficiencias, las limitaciones y las debilidades del método actual de registro que justifique que sea reemplazado por uno de reconocimiento facial. La información que tenemos es limitadísima", explica Valeria Betancourt, coordinadora del Programa de políticas de información y comunicación de la Asociación para el Progreso de las Comunicaciones, APC.

Respecto a los potenciales riesgos, Betancourt es clara: el sistema "Expone a la población más vulnerable a riesgos que son a todas luces desproporcionados. No solo por exacerbar las condiciones de discriminación con base a sesgos que tengan que ver con el color de la piel, prejuicios sociales, sino los riesgos a los que somete por el uso fraudulento, ilegítimo, político de los datos de estas personas".

En ese sentido, vale la pena recordar un episodio reciente: en septiembre se conoció la filtración de 18 GB de datos pertenecientes a prácticamente la totalidad de los habitantes de Ecuador,[20] incluyendo números de

16 Más información en https://derechosdigitales.tumblr.com/post/176557642641/vigilancia-en-el-metro-anuncian-sistema-de

17 Más información en https://agora.folha.uol.com.br/sao-paulo/2019/06/reconhecimento-facial-bloqueia-331-mil-bilhetes-unicos-em-sp.shtml

18 Más información en https://adcdigital.org.ar/portfolio/tu-yo-digital-descubriendo-las-narrativas-sobre-identidad-y-biometria-en-america-latina/

19 Más información en https://adcdigital.org.ar/wp-content/uploads/2019/05/ADC-Fintech-Argentina.pdf

20 Más información en https://www.bbc.com/mundo/noticias-america-latina-49721456

identificación y de teléfono, registros familiares y de trabajo. Para Betancourt, ese caso de muestra "que no hay capacidad en el sector público para hacer un manejo responsable, eficiente de los datos de los ciudadanos". Más todavía cuando Ecuador no cuenta con una ley de protección de datos personales que asegure límites basados en el respeto a los derechos fundamentales respecto al uso y aplicación de estos sistemas.

Además del proyecto liderado por el Ministerio de Inclusión Económica y Social, existen actualmente en Ecuador otros dos proyectos que están intentando implementar tecnologías de reconocimiento facial. El primero de ellos busca generar un sistema de videovigilancia orientado a mejorar las condiciones de seguridad de la ciudad de Quito, utilizando a la capital como una experiencia piloto con intenciones de expandirse al resto del país. El segundo, es una iniciativa de la estrategia Ecuador Digital, que está liderada por el Ministerio de Telecomunicaciones y Sociedad de la Información, y que apunta a agilizar los procedimientos alrededor de los trámites en el sector público.

Respecto a las motivaciones detrás de estos proyectos, Betancourt señala que "se piensa que la implementación de estos sistemas de por sí va a resultar un incremento de la eficiencia en los servicios o que de por sí van a mejorar las condiciones de seguridad en los espacios públicos, cuando lo que hemos visto es que si se aplican en las condiciones en las que hemos referido resultaría mucho más problemático que parte de una solución. La implementación de estos sistemas sin una mirada de derechos humanos es terriblemente problemática".

Esta es solo una muestra del modo en el cual las tecnologías de reconocimiento facial se están implementando por la región. No son los únicos: países como México y Brasil – que utilizó un sistema de reconocimiento facial para vigilar a los participantes de la más reciente edición del Carnaval de Río de Janeiro – están implementado sistemas de este tipo a diferentes escalas y con propósitos diversos, ya sea a nivel de gobierno central o local, e incluso a veces en manos de privados, como en el caso chileno. Y no sería del todo extraño que entre el momento en que se termine de escribir este texto y su posterior publicación, una nueva iniciativa haya sido anunciada en Perú, Panamá o Uruguay.

En el intertanto, la ADC ha introducido una Acción Declarativa de Inconstitucionalidad contra el Gobierno de la Ciudad de Buenos Aires por la resolución que introduce el sistema de reconocimiento facial. TEDIC, junto al Instituto de Derecho y Economía Ambiental (IDEA), presentó una acción de inconstitucionalidad contra las resoluciones que negaron las solicitudes de información sobre el sistema de reconocimiento facial. Por su parte, tanto en Bolivia como en Ecuador se están estudiando los siguientes pasos a seguir en la materia.


DERECHOS
DIGITALES
América Latina