El reconocimiento facial no pertenece a nuestro espacio público

En la Ciudad de Buenos Aires se ha implementado desde 2019 el "Sistema de Reconocimiento Facial de Prófugos" (SRFP) cuyas características lo vuelven altamente intrusivo y una amenaza para los derechos de los ciudadanos. Su despliegue se hizo a través de una resolución administrativa y con ausencia de intervención de la Legislatura. De esta manera, la norma no cumplió con el principio de legalidad requerido como condición necesaria –aunque no suficiente– para restringir derechos fundamentales. El Proyecto de Ley 1686-D-2020 pretende abordar esta situación, sin embargo, consideramos que hay razones suficientes para que la Legislatura proteja a la ciudadanía de esta tecnología de vigilancia masiva.

Frente a esta situación, desde la Asociación por los Derechos Civiles (ADC) aconsejamos dejar de utilizar, y suspender en el futuro inmediato, cualquier implementación de tecnologías de reconocimiento facial con fines de vigilancia en el espacio público. La razón fundamental es que el estado actual de dicha tecnología, junto con una legislación general inadecuada para afrontar los desafíos del procesamiento biométrico, resultan obstáculos insalvables para cualquier iniciativa que pretenda respetar nuestros derechos.

A continuación exponemos un breve análisis con los fundamentos centrales de nuestra visión.

Al poco tiempo de la implementación del SRFP, comenzaron los casos de personas identificadas erróneamente como prófugas. Por ejemplo, a fines de julio de 2019, Guillermo Ibarrola venía de pasar un día en familia en un fin de semana cotidiano. El día cobró un giro inesperado cuando Guillermo fue detenido, luego de pasar por los molinetes en la estación de trenes de Retiro, al salir del andén. Oficiales de la Policía Federal le informaron que tenía que acompañarlos a una dependencia policial. Lo que Guillermo nunca podría haber imaginado es que los próximos **seis días quedaría preso**, trasladado a un penal en Bahía Blanca, acusado de un delito que no cometió.

El caso de Guillermo no había sido el único. El mes anterior, mientras Leo Colombo Viña volvía a su oficina en un día laboral corriente, fue demorado en el andén de la estación Callao del subte. Las múltiples acreditaciones de su identidad no fueron suficientes para convencer a los oficiales de la Policía de la Ciudad que no era a quien estaban buscando y que había un error. Leo fue liberado luego de varias horas perdidas en la comisaría para esclarecer la

situación frente al juzgado. Horas y estrés producido por la situación que no podrán recuperarse.

Historias similares a las de Guillermo y Leo se han repetido. Como Daniel Frey, quien aún debe transitar con un certificado del Juzgado y con miedo de subirse al transporte público por si lo vuelven a detener. O el de una señora detenida 10 horas por una causa prescripta donde no se presentó como testigo, quien no solo sufrió la angustia al ser trasladada desde el andén esposada, sino tener que soportar los gritos de "chorra" por otros pasajeros.

El "Sistema de Reconocimiento Facial de Prófugos" (SRFP) no solo ha potenciado la vigilancia del espacio público como nunca antes; además **ha puesto en jaque las mismas garantías Constitucionales** que el Estado debe resguardar y asegurar.

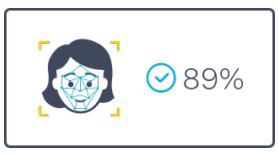
El Gobierno de la Ciudad de Buenos Aires impuso un sistema que vulnera múltiples derechos. Implementó esta tecnología esquivando la discusión pública sobre cómo queremos desarrollar nuestra vida en sociedad bajo vigilancia, y peor aún, no llevó a cabo los análisis de impacto en derechos humanos, necesarios para comprender cabalmente la manera en que se vulneran esos derechos.

Como legisladoras y legisladores, tienen en sus manos la posibilidad de revertir mayores menoscabos en la construcción de una sociedad más justa, más libre y más democrática.

¿Qué es el reconocimiento facial y por qué es problemático?

El reconocimiento facial es una tecnología biométrica que permite reconocer e identificar a las personas mediante sus rasgos faciales.

Los datos biométricos están íntimamente vinculados a nuestra identidad, ya que forman parte de quiénes somos como persona, nuestras características y comportamientos. **Estos rasgos se quedan con nosotros durante toda nuestra vida.**



El reconocimiento facial funciona mediante un software (con un algoritmo) que reconoce rostros e individualiza sus rasgos mediante una plantilla, que contiene por ejemplo la distancia entre los ojos, la nariz y la boca, etcétera. Esta tecnología, como toda la biometría, implica un proceso de probabilidades, el sistema no es infalible. Su propósito es indicar en qué porcentaje la plantilla de un rostro se parece a otro.

Para conocer más detalles sobre cómo funciona el reconocimiento facial y cómo se procesan los datos biométricos, puede visitar:

🌐 **https://conmicarano.adc.org.ar**

El próximo paso para proteger nuestra democracia: prohibir el uso del reconocimiento facial para la vigilancia por fuerzas de seguridad

En su estado actual de madurez, el reconocimiento facial presenta serios problemas y desafíos. No solo para los derechos a la privacidad y la protección de datos personales, sino también para garantías constitucionales como la presunción de inocencia y el debido proceso, los derechos a la no discriminación, a la libertad de expresión, de reunión y de asociación. Al mismo tiempo, cambia completamente cómo entendemos y disfrutamos del espacio público.

1. **Facilita un nivel de vigilancia masiva y automatizada nunca antes visto en democracia:** los algoritmos de reconocimiento facial deben necesariamente detectar todas las caras que ven las cámaras en donde están implementados. Por más que el nombre de una persona no esté vinculado a su rostro, el software igualmente detectará su cara.

2. **Discriminación**: El entrenamiento del algoritmo define la precisión con la cual podrá reconocer rostros en diversos escenarios. En esta etapa de entrenamiento es donde aparecen los sesgos que pueden resultar en la discriminación de una persona o, peor aún, culpar a alguien de un crimen que no cometió.

   Esto ocurre porque los algoritmos de reconocimiento facial pueden tener errores al reconocer mal a una persona por tener rasgos "parecidos" a otra, por ejemplo debido a su tez o género. Esto se conoce como falsos positivos.

   La tecnología biométrica, como el reconocimiento facial, funciona en base a probabilidades. El sistema brinda un porcentaje de qué tan parecida es la persona identificada de aquella a la que se busca. Este resultado nunca será del 100%, por lo cual quien implementa el sistema debe decidir qué porcentaje considera aceptable.

3. **Revierte la carga de la prueba, violando la presunción de inocencia**: Esto se suma a los problemas sobre la acusación de personas inocentes por las

deficiencias técnicas. Todas las personas que pasen frente a la cámara son culpables hasta que el sistema 'descarte', por sus rasgos faciales, que no son a quienes se busca.

4. **Uso encubierto y sin consentimiento**: Por la manera en la que funciona el reconocimiento facial, las personas que transitan frente a las cámaras de videovigilancia no se enteran que se está realizando un proceso de identificación con sus datos biométricos. Asimismo, el reconocimiento facial también puede realizarse sobre grabaciones de video o fotografías pasadas.

   Incluso si se colocara un cartel cerca de la cámara para avisar del uso, al momento de llegar a leerlo de cerca, sus datos biométricos ya habrán sido procesados.

   A esto se suman los problemas de consentimiento cuando se usa el reconocimiento facial en la vía pública. La persona que no desee someterse a esta intromisión solo tiene como recurso evitar transitar por las zonas donde la tecnología está en uso. Esto interfiere directamente con la libertad de circulación y el acceso al transporte público, en el caso de CABA. **Afectando a su vez el derecho a la libre reunión, asociación y expresión, al producir un efecto inhibitorio en el comportamiento de las personas que son observadas.**

5. **El tratamiento de datos sensibles**, como los datos biométricos, aumenta el riesgo ante filtraciones o vulneraciones a la base de datos, debido a una pobre o nula implementación de medidas de seguridad informática. En los últimos años se han conocido múltiples casos[1] donde el Estado no tomó los recaudos necesarios. A esto se suma que el país aún no cuenta con políticas extensas en materia de ciberseguridad.

6. **Se distorsiona el propósito original de la recolección de datos**: Mientras las personas deben dar sus datos biométricos para obtener su DNI o pasaporte, esos mismos datos luego pueden ser utilizados en su contra, alterando el propósito original y al mismo tiempo perjudicando la confianza sobre los organismos públicos existentes.

Además de los problemas intrínsecos a la tecnología en sí, el Sistema de Reconocimiento Facial implementado en Buenos Aires debe analizarse de forma íntegra, con todos sus elementos y contexto.

[1] El caso más paradigmático ocurrió en 2019 contra la Policía Federal Argentina.

Previo a la implementación del SRFP, el Gobierno de la Ciudad debería haber realizado una evaluación de impacto para determinar las bases y justificación de la necesidad y proporcionalidad del mismo.

Según consta en las solicitudes de información pública presentadas por la ADC, este proceso no se llevó a cabo. Ello fue confirmado además por el Relator Especial de Naciones Unidas por el derecho a la privacidad, quien tras su visita al país publicó un comunicado crítico con sus conclusiones.

La construcción de políticas públicas no puede pensarse desde la solución para luego identificar el problema que se busca resolver. El GCBA debería haber estipulado, con evidencia empírica, las diversas medidas posibles para resolver el problema de fondo que menos interfieran y socaven derechos fundamentales, para luego descartarlas si no fueron útiles.[2] Mas aún ante la problemática de seguridad pública que aflige a los habitantes del suelo argentino a diario.

¿Cuál es la tendencia en el resto del mundo?

En junio de 2019, el Relator Especial de Naciones Unidas por el derecho a la libertad de expresión expuso frente al Consejo de Derechos Humanos la necesidad de que los Estados establezcan moratorias inmediatas al uso de tecnologías de vigilancia (incluyendo el reconocimiento facial), hasta que se sancionen regulaciones ajustadas al marco de derechos humanos, con extensas salvaguardas.

Entre 2019 y lo que llevamos de 2020, múltiples ciudades en Estados Unidos han aprobado una regulación local para prohibir que la policía y las fuerzas de seguridad utilicen tecnologías de reconocimiento facial para vigilar el espacio público.

En el estado de California, una ley prohíbe el uso en las cámaras colocadas en los chalecos de oficiales de policía. Además, varias ciudades prohibieron el uso mediante ordenanzas municipales: San Francisco, Berkeley, Oakland, Alameda. En el estado de Massachusetts, también se sancionaron ordenanzas en las

[2] El sistema interamericano se ha remitido a la Declaración Conjunta sobre la libertad de expresión y las respuestas a las situaciones de conflicto, que enfatiza que "de acuerdo con el triple test para las restricciones a la libertad de expresión y, en particular, la parte de necesidad de ese test, la vigilancia debería llevarse a cabo solo de forma limitada y selectiva y de una manera que represente un equilibrio adecuado entre el orden público y las necesidades de seguridad, por un lado, y los derechos a la libertad de expresión y a la privacidad, por el otro. La vigilancia indirecta o masiva, es inherentemente desproporcionada y constituye una violación de los derechos de privacidad y libertad de expresión...". párrafo 223: http://eduteka.icesi.edu.co/pdfdir/oea-cidh-estandares-para-una-internet-libre.pdf

ciudades: Easthampton, Boston, Springfield, Cambridge, Northampton, Brookline, Somerville.

Por otra parte, en agosto 2020 en el Reino Unido, la Corte de Apelaciones falló a favor de una demanda contra el uso de reconocimiento facial en vivo por la Policía de Gales del Sur. La Corte estableció que el reconocimiento facial es una tecnología más invasiva que la simple captura de fotografías o el uso de cámaras de videovigilancia (CCTV). Determinando además que no existen actualmente los marcos jurídicos necesarios para ser utilizada por la policía, y que la implementación se realizó sin cumplir correctamente con las evaluaciones de impacto en la privacidad y los sesgos del sistema.

Además del ámbito legislativo y judicial, a comienzos de junio de 2020, tres de las empresas tecnológicas más grandes del mundo anunciaron que dejarían de ofrecer sus productos de reconocimiento facial a la policía y fuerzas de seguridad. IBM, Amazon y Microsoft reafirmaron la necesidad de un abordaje de derechos humanos para el uso de esta tecnología invasiva.

El rol del Poder Legislativo es clave para limitar y prohibir abusos de derechos fundamentales mediante el uso del reconocimiento facial

Reafirmamos la necesidad de la discusión pública sobre el uso de esta tecnología. Sin embargo, consideramos que antes de apresurarnos a incorporar legalmente un sistema impuesto de forma unilateral, se debata sobre los aspectos esenciales vinculados al mismo.

La actualización de la Ley 1845 de Protección de Datos de la Ciudad de Buenos Aires, la realización de una evaluación de impacto en derechos humanos sobre el SRFP, incrementar la transparencia sobre la industria de la vigilancia y su rol en las estrategias de política criminal del Poder Ejecutivo, **son todas deudas que no han sido saldadas y deberían tratarse previo a la introducción del reconocimiento facial mediante una ley**.

Por ello, alentamos este debate público, donde se puedan convocar expertos y múltiples voces, para primero definir qué implican las actividades de vigilancia masiva en nuestros espacios públicos y su interferencia con derechos fundamentales.