

BRIEFING SOBRE BIOMETRÍA PARA PERIODISTAS

Abril 2019

- ¿Cuál es la situación?

- [El Estado pretende utilizar tecnología biométrica](#) (específicamente de reconocimiento facial) con fines de investigación criminal en la vía pública.

- ¿Qué hace la Asociación por los Derechos Civiles?

- Desde hace al menos siete años que trabajamos en el monitoreo de las políticas públicas que implementan tecnología de identificación biométrica, llevando a cabo investigaciones, análisis legales y proponiendo recomendaciones a funcionarios y legisladores. Ante el reciente anuncio del uso de reconocimiento facial en el espacio público porteño, [presentamos una solicitud de acceso a la información pública](#) para instar al Estado a que brinde explicaciones detalladas sobre todos los aspectos del proyecto. Particularmente, el impacto en la privacidad y la libertad de expresión, la potencial discriminación a grupos vulnerables y las medidas de control y rendición de cuentas para evitar abusos.

Reconocimiento facial en la CABA

a) La biometría no se encuentra contemplada por ley

En Argentina, no hay una ley que establezca expresamente el uso de tecnologías identificación biométrica, ni a nivel nacional ni en la Ciudad Autónoma de Buenos Aires.

Es importante destacar que prácticamente todas las implementaciones de tecnología biométrica en el país que ya se encuentran operativas (por nombrar los principales sistemas y bases de datos: SIBIOS; la base de datos de RENAPER y la emisión del DNI y el pasaporte, junto con su uso en Migraciones; el Sistema de Identidad Digital; las bases de datos de ANSES y de la AFIP) se llevaron a cabo por decretos del poder ejecutivo o resoluciones ministeriales.

La implementación de biometría en la Argentina se ha justificado principalmente mediante el decreto-ley 17.671 “de identificación, registro y clasificación del potencial humano nacional”, que tanto en su contenido como en su forma es altamente poco democrático. El decreto-ley fue sancionado durante la dictadura militar de Onganía, y los gobiernos democráticos en los últimos años no hicieron más que naturalizar su

aplicación. La ley 17.671 no contempla el uso de “biometría” expresamente, solo habla de fotografías y dactiloscopia, que en términos de tecnología no son lo mismo.

A nivel jerárquico, tanto decretos como resoluciones se encuentran por debajo de la ley. Esto es importante porque según la Constitución y los tratados internacionales de DD.HH., para implementar cualquier tipo de limitación a un derecho, es necesario hacerlo por vía de una ley sancionada por el órgano legislativo, la cual debe contemplar la finalidad/ necesidad específica a la que apunta el Estado y esa medida debe ser proporcional teniendo en cuenta el / los derecho/s que se limita/n.

En este caso, la medida claramente es desproporcionada si su finalidad es perseguir la comisión de hurtos.

Lamentablemente, la Argentina no está sola en esto, ya que la gran mayoría de los países en América Latina siguen la misma lógica: implementar tecnología por vía de decretos o resoluciones, esquivando el debate público.

b) El uso de reconocimiento facial redefine lo que entendemos por espacio público, restringiendo libertades

Nuestra posición desde la ADC es desaconsejar el uso de la biometría en el espacio público, pues consideramos que los riesgos en la implementación de esta tecnología no superan a los potenciales beneficios que pueda traer.

El reconocimiento facial es una de las tecnologías más debatidas en la actualidad cuando se la pretende utilizar con fines criminales y/o en el espacio público.

Debido a que la biometría es un proceso de estadística, donde se trata de encontrar un balance entre las tasas de error (falsos positivos y falsos negativos) para poder identificar correcta o incorrectamente a una persona, nunca es fiable en un cien por ciento.

Los algoritmos de reconocimiento facial, que son los que implementan dichas tasas de error, pueden estar programados con determinados sesgos (incluso en forma involuntaria; no olvidemos que casi todo lo que

consumimos en tecnología está desarrollado predominantemente por hombres blancos). El resultado es la discriminación de aquellos grupos históricamente vulnerables, en particular los conformados por las personas no binarias, trans, queer, gender fluid o las que no tienen tez blanca.

El uso de la biometría en el espacio público redefine no solo cómo vemos dichos espacios, sino -todavía más preocupante- la utilización que haremos de ellos.

Como personas tenemos derecho a una expectativa de privacidad en la vía pública.

Cuando caminamos por la vereda, un parque o nos movemos en transporte público, no nos desplazamos con un cartel que le grita a todo el mundo quién somos, a dónde vamos o de dónde venimos, dónde vivimos, de qué trabajamos.

¿Por qué es razonable esa expectativa? Porque podemos asumir que cuando estamos en estos espacios públicos, las personas con las que los compartimos no están interesadas en nosotros, y saber cualquier tipo de dato personal de nuestra vida requiere de un esfuerzo proactivo considerable por parte de quien lo busca.

Toda esta situación cambia cuando se implementa el reconocimiento facial en la vía pública, porque sabiendo por dónde transitan las personas no solamente se está interfiriendo con su derecho a la privacidad, sino además coartando la libertad de expresión, reunión y asociación.

Las personas modifican o alteran su comportamiento cuando tienen un mínimo presentimiento o sospecha de que están siendo observadas o vigiladas. Lo que antes podía ser una plaza para el intercambio social y cultural, donde los individuos tienen la posibilidad de expresarse para el desarrollo de su identidad y personalidad, puede convertirse en un espacio de opresión.

c) ¿Qué debería hacer el Estado cuando se plantea el uso de tecnología con fines de seguridad pública?

- Realizar estudios que permitan obtener evidencia científica para saber con certeza cuál es el problema que se pretende solucionar. Esto debería

incluir cuáles son las posibles soluciones y medidas a tomar, ya que el Estado debe optar siempre por aquellas menos intrusiva en los derechos de los ciudadanos.

- Recién una vez obtenida dicha evidencia podemos hablar de empezar un debate legislativo y público, para que toda la sociedad pueda ser parte y hacer oír la voz de los expertos con las advertencias y recomendaciones del caso puntual.
- Para evitar abusos, la legislación debe contener estrictas previsiones sobre transparencia, rendición de cuentas y supervisión/control.

d) ¿Qué ocurre con los datos biométricos?

Aún con todo lo descrito antes, el uso de la biometría desde un punto de vista tecnológico y de datos personales es sumamente sensible.

Los datos biométricos no se pueden cambiar. Esto implica que ante una filtración de la base de datos, miles o millones de personas van a encontrarse vulnerables a potenciales abusos y daños personales.

Lógicamente en lo que respecta a seguridad informática, el estándar en la transmisión y almacenamiento de la información es implementar algoritmos de cifrado (igualmente esto depende de su correcta implementación y uso, qué certificados se usa, cómo se manejan las llaves para cifrar y descifrar la información, etcétera).

Respecto al software de reconocimiento biométrico, no solo es necesario conocer quién lo desarrolló, sino además evaluar -para evitar que existan posibles backdoor- si se llevaron a cabo auditorías, idealmente independientes, de seguridad.

Otro estándar en lo que respecta a seguridad de la información es el concepto de minimización. Es decir, recolectar la cantidad mínima indispensable de los datos para que el sistema funciona. Pero tengo mis reservas sobre cómo se podría implementar eso efectivamente en un sistema que por su fin tiene previsto vigilar el flujo de personas.

Recursos

- 1 - *La identidad que no podemos cambiar. Cómo la biometría afecta nuestros derechos humanos* (ADC, abril de 2017).
- 2 - *Cuantificando identidades en América Latina. Un breve repaso acerca de cómo las sociedades latinoamericanas se enfrentan a la implementación de las tecnologías biométricas* (ADC, mayo de 2017).
- 3 - *Desafíos de la biometría para la protección de datos personales* (ADC, mayo de 2017).

