uchile.cl

# Pandemia y tecnología: los riesgos del reconocimiento facial

*Texto: Felipe Ramírez Prensa-UChile*

6-7 minutos

---

El fracaso de la aplicación de reconocimiento facial implementada por el Registro Civil para entregar la "clave única" a la ciudadanía sin necesidad de que acudieran presencialmente a una sucursal, alertó sobre los riesgos de sistemas tecnológicos que aún cuentan con bajos niveles de fiabilidad, y reinstaló el debate sobre la ciberseguridad y el uso de datos sensibles de personas. Daniel Álvarez, académico de la Facultad de Derecho, y Jorge Pérez, profesor de la Facultad de Ciencias Físicas y Matemáticas e investigador del Instituto Milenio Fundamentos de los Datos, analizaron las falencias y riesgos de este tipo de innovaciones.

El uso de tecnologías de vigilancia como el reconocimiento facial o aplicaciones en teléfonos móviles para supervisar la cuarentena de personas contagiadas con COVID-19 en algunos países asiáticos, puso sobre la mesa diversos debates relacionados al resguardo de datos personales y su equilibrio con la seguridad.

En nuestro país, esta discusión aterrizó tras el fracaso de un **sistema de reconocimiento facial implementado por el Registro Civil** para evitar que las personas debieran asistir presencialmente a sus oficinas para activar su "clave única" en el contexto de la cuarentena de siete comunas de la capital.

**La app generada para este efecto fue burlada el mismo día de su puesta en funcionamiento por un usuario**, que demostró lo fácil que resultaba engañar el sistema para obtener la clave de otra persona utilizando una imagen descargada desde internet, por lo que fue retirada al poco tiempo.

El académico del Departamento de Ciencias de la Computación, **Jorge Pérez**, explicó que una de las dificultades para analizar este y otros usos de esta tecnología radica en el desconocimiento del código detrás de cada una.

Precisamente este aspecto es preocupante en lo sucedido con el Registro civil, ya que **"si hablamos de un organismo público debería haber total transparencia sobre los métodos que se han utilizado. Mientras no sepamos eso, sólo se podrá inferir lo que pasó, y se hace muy difícil una auditoría**

**independiente".**

Consultado sobre la experiencia en países asiáticos, el académico recordó que no se conoce a ciencia cierta cuál es la efectividad de las herramientas de reconocimiento facial que se usan en otros países, debido al desconocimiento del código y el detalle de su implementación, pero que **la información disponible apunta a una baja efectividad.**

"Un punto importante es que para un sistema de este tipo necesitas fotos para contrastar, una base de datos, entonces si ese banco es de mala calidad vas a tener muchos errores. Lo que yo entiendo es que el gobierno como mucho tiene disponible la foto de la cédula de identidad, que es de baja calidad, por lo que puede fallar", profundizó Pérez.

Pero más allá de la efectividad que tenga esta tecnología, el también investigador del Instituto Milenio Fundamentos de los Datos remarcó que hay lugares como California donde está siendo prohibida por violar derechos fundamentales a la privacidad. **"Hay una discusión que no hemos tenido al respecto. Yo personalmente estoy en desacuerdo con las cámaras de vigilancia y reconocimiento facial en la calle, me parecen inadecuadas para tomar decisiones públicas**", aseguró Pérez.

Para el profesor Daniel Álvarez, de la Facultad de Derecho, el tema más preocupante no tiene que ver con el reconocimiento facial, una tecnología que asegura tiene un nivel de madurez bajo, sino que con **la falla de seguridad respecto a la entrega de la "clave única".**

"Este es un instrumento que el Estado desarrolló para que por medio de plataformas digitales, las personas puedan realizar una gran cantidad de trámites en instituciones públicas, y **su vulneración representa un riesgo de ciberseguridad mayor**", afirmó el académico.

El experto destacó que **el filtro para la verificación de la identidad a la hora de activar esta clave radicaba en la petición física del trámite, por lo que al eliminarse desapareció la principal herramienta para evitar suplantaciones de identidad**, reemplazándose por un sistema inseguro y poco idóneo. "No se tiene que caer en el idealismo tecnológico. Es cierto que la tecnología puede resolver un montón de problemas, pero cuando están maduras, en cambio probar en un contexto de excepcionalidad tecnologías inmaduras que pueden llegar a un 95 por ciento de error, es generar más riesgos", afirmó.

A ello se suma que cuando la aplicación se instalaba, solicitaba permisos en los aparatos que calificó de "desproporcionados", que

incluía información sensible de las personas, y que era manejada por una tercera compañía, que además podía acceder a la base de datos del Estado, sin el consentimiento del usuario para ninguna de esas cosas. "Surge la duda entonces si el tratamiento de estos datos recolectados se realizó en Chile o en el extranjero, al ser una empresa internacional, y si sus procedimientos se ajustan o no a la ley", alertó.

Consultado sobre si en nuestro país es posible imaginar sistemas de rastreo de contagiados por COVID-19 como se ha realizado en otros países, **el profesor Álvarez explicó que si bien el Ministerio de Salud puede tratar datos personales de personas contagiadas por una enfermedad, ello no podría ser delegado al Ministerio del Interior y Seguridad Pública**, ya que no está entre sus atribuciones legales.

"**Esta es una materia que algunos países asiáticos tienen bastante reglado, y hay que tener en consideración que son regímenes democráticos distintos. China puede hacer lo que hace porque es un gobierno autoritario donde los derechos de las personas están por debajo de las necesidades del Estado**, situación que es al revés en Occidente. Pero este es un debate muy interesante que debe darse a propósito de lo que viene luego de esta crisis", finalizó.