latercera.com

¿Podemos confiar en sistemas de reconocimiento facial como el del Registro Civil? - La Tercera

La Tercera

10-13 minutos

Este domingo, el **Registro Civil** lanzó una aplicación en línea que buscaba eliminar, **teóricamente**, la obtención de la **Clave Única**, útil para todo lo relacionado con servicios del Gobierno, así como **permisos vinculados a la cuarentena** por la pandemia de coronavirus que afecta al país. La idea era autenticar la identidad del usuario empleando la cámara, y solucionar el problema generado en los últimos días para quienes buscaban realizar el trámite.

Sin embargo, horas después un usuario de Twitter demostró **con un sencillo experimento**, que el sistema se podía burlar fácilmente con **una foto**, una **base de datos del RUT** disponible en internet, y algo de ingenio. Ante las evidencias, el Registro Civil optó por **bajar la aplicación**, aduciendo que la empresa encargada mejoraría el problema.

“Ante algunos problemas que ha presentado la aplicación para obtener #ClaveÚnica momentáneamente no está disponible. @IdemiaGroup la empresa desarrolladora de la app está trabajando para dar una pronta solución”, anunció el organismo.

Entonces, **¿son estos sistemas confiables?**

El primer antecedente de un registro “biométrico” lo tenemos **en 1888**, cuando **Alphonse Bertillon**, un oficial de policía francés, tuvo una sencilla pero ingeniosa idea: identificar criminales en base a sus características físicas, creando una ficha con un total de 11 mediciones, una descripción y retratos fotográficos. Pasarían **más de 100 años** hasta que **Joseph Atick**, un experto en la materia, daba a conocer los primeros indicios de un computador analizando rostros de la misma forma en que lo hacía un cerebro humano, describiendo los principios que hoy, **más de 25 años después**, se siguen utilizando en algo tan cotidiano como un smartphone.

Porque a pesar de sus limitaciones, el mercado de esta tecnología sigue creciendo, con un estimado de **4,5 mil millones de dólares en 2018**, esperando alcanzar los **9 mil millones de dólares para 2024,** con EE.UU. y China como sus mayores exponentes.

A estas alturas, **todos los teléfonos de alta gama** cuentan con un modo de desbloqueo facial, aunque varían en su implementación dependiendo de **la forma de "medir" la profundidad del rostro**. Mientras **Apple** usa en sus iPhone la tecnología de Kinect de Xbox, los modelos de **Samsung, Huawei** y **LG** emplean algo llamado "Time of Flight", un sistema de sensores que funciona de la misma forma que **un radar o al sonar de un submarino**.

Técnicamente, **Apple** asegura que su desbloqueo facial llamado Face ID es más seguro (falla 1 en 1 millón vs 1 en 50 mil del detector de huellas), y a su vez, **Huawei** y **Samsung** afirman que la combinación de iris y cámara es mejor, o bien el reconocimiento dactilar es "más intuitivo".

Como sea, en el fondo todos **buscan evitar** lo ocurrido con la foto de Daniel Matamala y la aplicación del Registro Civil.

Para el **abogado y presidente del Consejo para la Transparencia (CPLT), Jorge Jaraquemada,** "lo ocurrido con la herramienta del Registro Civil es muy grave. El disponer de reconocimiento facial para acceder a la Clave Única **va en contra de los estándares de seguridad** que el Estado debe tener en post de una óptima protección de un dato personal como el rostro de una persona".

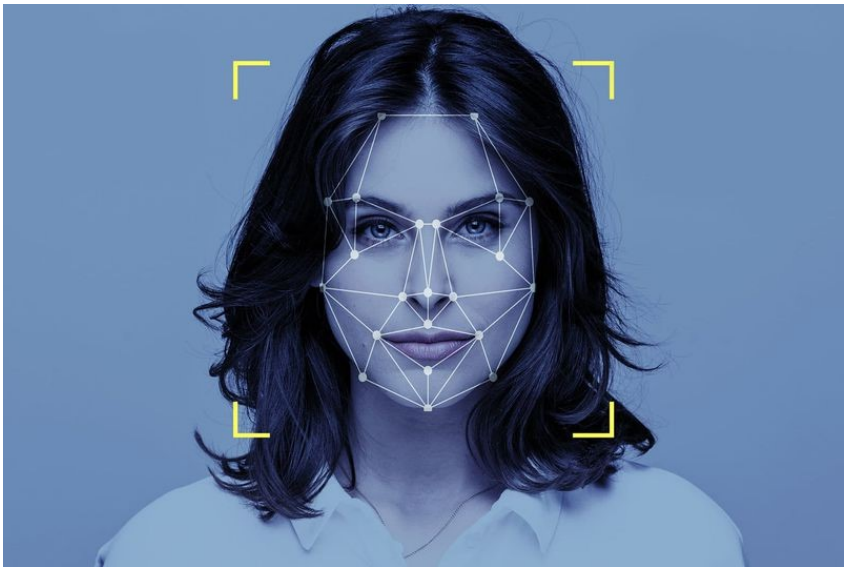
"El desarrollo de herramientas que faciliten a las personas solicitar por vía remota su clave única **no puede implicar un relajo de los altos estándares de ciberseguridad**", añadió, puntualizando que **la clave en sí misma es un dato personal**, y además es la "llave de acceso" a diversa información relacionada con el titular, incluyendo otros datos personales como el nombre y de carácter sensible como el estado de salud, además de otro tipo de información privada de las personas.

El presidente del CPLT enfatiza en la necesidad que "todos los procesos asociados a la clave única, en particular su entrega, requieren la adopción de un enfoque proactivo y preventivo de **ciberseguridad y privacidad**, desde su diseño", apuntando a la necesidad de analizar "con especial cuidado, todos los riesgos que la operación de esta herramienta conlleva, aplicando medidas de seguridad efectivas y proporcionales para abordarlos".

Asimismo, Jaraquemada también critica el que se opte por una tecnología como el perfil biométrico para un fin que **podría conseguirse con otro tipo de datos** que permitan confirmar la identidad del solicitante de la clave.

"Este tipo de situaciones suma aristas que pueden ser problemáticas a una medida excepcional que debe implementarse en corto tiempo, generando incertidumbre en la ciudadanía".

"Nuestro llamado como Consejo es buscar **un mecanismo que sea más proporcional y adecuado con el objetivo** que se busca, además de informar adecuadamente –a través de las políticas de privacidad- cómo se resguardarán y usarán estos datos por parte de la entidad", comenta.



Eduardo Graells-Garrido, investigador del Barcelona Supercomputing Center e Instituto de Data Science UDD, puntualiza que "a diferencia de las personas, en general las máquinas **sólo pueden identificar lo que les enseñaron** y **en las condiciones** en las que les enseñaron".

"Estos sistemas funcionan con las distintas características que vio en millones de fotos de rostros, tratando de identificarlas. Éstas incluyen los colores de la foto, por tanto: colores de piel, de ojo, de pelo, distribución de elementos en el rostro, como los ojos, los pómulos, la boca, partes que tienen posiciones relativas a las otras, determinadas por la anatomía humana; si la calidad de imagen lo permite, las texturas (como la rugosidad de la piel, que no es la misma de una máscara de plástico); entre otras. En el caso de las **redes sociales**, también hay información contextual: en la foto de una fiesta es probable que las personas que aparezcan juntas se conozcan y sean -o aparente ser- amigas, reduciendo el campo de candidatas a ser identificadas".

Entonces, **¿qué podría salir mal?**

Graells-Garrido comenta que reconocer que una foto contiene un rostro, y saber a quien pertenece, es **un problema de clasificación** que las máquinas pueden resolver bien si se pide reconocer a quienes aparecen en fotos de las mismas características donde se aprendió.

"Si la máquina lo hizo estudiando fotos de frente de alta resolución con buenas condiciones de iluminación, y en vez de eso le entregamos fotogramas de un video a baja resolución, con un

ángulo superior de encuadre, en condiciones de paupérrima iluminación, **el resultado será basura**. Pero la máquina **responderá igual**, ya que una característica de los algoritmos es que **pocas veces dicen que no saben la respuesta**".

"Técnicamente, hay que aclarar que las máquinas ven, **pero no es el mismo ver nuestro**. Si la máquina aprendió solamente con fotos de perfil de redes sociales, no reconocerá rostros, reconocerá fotos de perfil de redes sociales. Si la máquina aprendió a ver fotos de personas de tez blanca o clara, no reconocerá a quienes tienen la piel más oscura", enfatiza.

Además de los problemas prácticos de la tecnología, otro tema complejo es **la privacidad de los datos biométricos de los usuarios**.

Jorge Jaraquemada explica que la actual **Ley N°19.628**, sobre tratamiento de datos personales, **no se refiere expresamente a los datos biométricos**, ni a su tratamiento en particular.

"Sin embargo, atendida la definición de datos sensibles contenida en la ley, de acuerdo a la cual, entre otros, considera como dato sensible las características físicas de las personas, un dato biométrico debe ser considerado como **un dato sensible a la luz de nuestra legislación vigente**. De esta manera, el tratamiento de estos datos (lo que incluye su comunicación, transferencia, almacenamiento, etc.) se debe realizar al amparo de lo dispuesto por la Ley mencionada, en tanto dichos datos deben ser considerados como un dato sensible de su titular", afirma.

"De esta manera, los datos sensibles no pueden ser objeto de tratamiento, salvo 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. Si no concurre alguna de las hipótesis descritas, **no podrá efectuarse tratamiento de los datos biométricos**", añade.

Aún así Jarquemada indica que en la actualidad **se discute en el parlamento** un proyecto que reforma la señalada Ley N°19.628.

En dicho proyecto, que se encuentra **en primer trámite constitucional en el Senado**, se contempla expresamente una regulación relativa a los datos personales biométricos, definiéndolos como “aquellos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona, que permitan o confirmen la identificación única de ella”. Además, señala expresamente, los casos en los cuales podrán tratarse dichos datos.

Asimismo, es por la falta de una ley relacionada que actualmente **no existe fiscalización por el uso de estos datos, ni su almacenamiento por terceros**.

“En este sentido, respecto de los datos biométricos que son tratados por los órganos de la Administración del Estado, **es el Consejo para la Transparencia** quien tiene la atribución de velar por el adecuado tratamiento de los mismos. Sin embargo, actualmente carecemos de facultades sancionatorias en caso de incumplimiento o de un tratamiento que no se ajuste a lo señalado por la ley”, explica Jaraquemada.

El experto recuerda que la ley entrega la facultad al titular del dato, para que éste pueda ejercer los derechos de **acceso, rectificación, cancelación y oposición** al tratamiento de sus datos personales y/o sensibles, incluyendo datos biométricos.

“En caso que el responsable del tratamiento del dato, no permita el ejercicio de dichos derechos, **el titular podrá recurrir al juez de letras en lo civil**, con el fin de hacer valer los derechos que le correspondan”, enfatiza.

Jorge Pérez, **investigador del Instituto Milenio Fundamentos de los Datos y académico del Departamento de Ciencias de la Computación de la U. de Chile**, afirma que básicamente, existen dos riesgos relacionados con esta tecnología: la **suplantación** -como ocurrió con Matamala-, y que las aplicaciones se realicen bajo contratos **que no protejan la privacidad**.

“No se puede saber la eficacia de estos sistemas mientras no se haga una auditoria exhaustiva, vale decir, **no sabremos cuántas suplantaciones posibles habrá por cada uso**”, señala.

En relación a la privacidad de los datos obtenidos por esta tecnología, Pérez indica que “la mejor forma es tener leyes que nos protejan, y votar por gente que considere estos temas como centrales en sus campañas”.

"Aunque a alguna gente le pueda parecer que es un problema secundario, la protección de datos, el derecho a la privacidad y a otras cosas como la total seguridad de comunicaciones privadas, **debieran de alguna forma consagrarse en la constitución**.

Tenemos la oportunidad única de pensar en una constitución para el futuro, para los próximos 50 o 100 años, e incluir estos temas es esencial", agrega.

"Otra buena forma es que Gobierno y Estado **se asesoren por gente técnicamente capaz** al momento de tomar decisiones de contratar tecnologías que afectan al público. Tenemos un Ministerio de Ciencia ahora y deberíamos usarlo".

"No podemos seguir dejando todas las desiciones y asesorías en entes privados. Tampoco podemos seguir dejando nuestros datos en manos de privados de manera indiscriminada. Y la forma de protegernos es con iniciativas generales, no con el cuidado que tengamos cada uno por separado el que nunca será suficiente", sentencia el académico.