



LA PROTECCIÓN DE DATOS BIOMÉTRICOS EN ARGENTINA

Autor: Abog Antonella Alejandra Rosato. COLEGIO DE ABOGADOS DE MORÓN.

SUMARIO. I. Introducción. II. Datos Biométricos. III.- Los datos biométricos como datos sensibles. IV.- Marco normativo en Argentina. V.- Derecho comparado. VI.- Uso de Datos Biométricos en Argentina VII.- Desafíos en la Protección de Datos Biométricos VIII.- Estafas con la utilización de datos biométricos. IX- Conclusiones.

I- Introducción

La protección de datos biométricos es un tema de creciente relevancia en el contexto actual, donde la tecnología avanza a un ritmo acelerado. En Argentina, la recopilación y el uso de estos datos plantean importantes desafíos en materia de derechos humanos y privacidad.

En el último tiempo, los riesgos en relación a la protección de los datos personales a través de la biometría han ido creciendo. La implementación de nuevas tecnologías implica un desafío para el derecho y para la protección de la intimidad de las personas.

Al día de hoy, la ley 25.326, la cual prevé la protección de los datos personales, a pesar de ser pionera en su momento, hoy resulta insuficiente dado el gran avance de la tecnología, el procesamiento de datos y las regulaciones dispuestas en otras regiones para el intercambio de estos.

El presente artículo pretende analizar el marco normativo argentino acerca de la protección de datos personales de carácter biométrico, el almacenamiento de los mismos, las tecnologías disponibles y plantear cuales serían las modificaciones necesarias de carácter legal para fortalecer el resguardo de estos datos.

II- Definición de Datos Biométricos

Los datos biométricos son aquellas características físicas, biológicas o de comportamiento que permiten identificar a una persona de manera única y permanente. Estos datos cuando son sacados de una persona son analizados y se almacenan en una base de datos o en un objeto de

posesión del individuo. Los mismos, se pueden comparar con las plantillas almacenadas para poder identificar a la persona.

A diferencia de otros datos personales, los biométricos no pueden ser alterados sin modificar la esencia de la persona, lo que plantea riesgos adicionales si son mal utilizados.

La ley de protección de datos de Argentina en su art 2 define los datos personales como toda *“información de cualquier tipo referidas a personas físicas (...) determinadas o determinables”*.

Esta definición amplia permite encuadrar a los datos biométricos como una especie de datos personales, ya que las tecnologías biométricas permiten la identificación “determinación” en el lenguaje de la ley argentina de las personas.

Por otra parte, el Reglamento (Ue) 2016/679 Del Parlamento Europeo Y Del Consejo nos da una definición específica de datos biométricos: como aquellos *“datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos”*¹

Existen dos tipos de datos biométricos, los datos biológicos y los datos de comportamiento. En cuanto a los datos biológicos, son aquellos que reconocen la fisiología de la persona como por ejemplo la retina o la huella digital.

En cambio, los datos de comportamiento son los que reconocen la forma de actuar de la persona, por ejemplo la firma o manera de clickear.

Existen hoy en día, muchas aplicaciones que utilizan estos datos para verificar la identidad en lugar del nombre de usuario y contraseña. Dentro de esta variedad podemos encontrar entre otros:

- Huellas digitales: La impresión que deja la yema del dedo en un objeto al tocarlo.
- Lectura de retina e iris: son tecnologías biométricas que se utilizan para identificar a una persona y que se caracterizan por ser altamente fiables y seguras. La principal diferencia entre ambas es la parte del ojo que se analiza y el método de captura de los datos. Por un

¹ REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, art 4.

lado, la lectura de retina analiza la retina y la capa de vasos sanguíneos que se encuentran en la parte posterior del ojo. Para ello, se utiliza una luz infrarroja de baja intensidad y un acoplador óptico que lee los patrones específicos. La precisión de esta técnica puede verse afectada por enfermedades que alteren la estructura de la retina. Y por otro lado, la lectura de iris analiza los patrones únicos del iris, la parte coloreada del ojo. Para ello, se utiliza una luz infrarroja invisible que ilumina el iris y una cámara especial que captura la imagen de los patrones. La estructura del iris es estable a lo largo de la vida, salvo en casos de lesiones graves en el ojo.

- Reconocimiento facial: es una aplicación dirigida por ordenador que identifica automáticamente a una persona en una imagen digital.
- Geometría de los dedos y mano: Se basa en la geometría de la mano, lo que requiere que el usuario coloque la mano de forma muy similar a la de la muestra inicial, complicando el uso del sistema. Además, existen métodos sencillos para engañar al sistema.
- Reconocimiento de voz: es un tipo de inteligencia artificial que tiene como objetivo permitir la comunicación hablada entre seres humanos y computadoras.

III- Los datos biométricos como datos sensibles

En el apartado anterior encuadramos a los datos biométricos como datos personales, sin embargo, debemos dar un paso más y preguntarnos si los datos biométricos no se encuadran dentro de una categoría especial de datos personales: los datos sensibles.

Según la definición de la ley argentina, se considera dato sensible los “*datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.*”² La sensibilidad de los datos biométricos radica en el hecho de que su uso indebido puede comprometer gravemente la privacidad y los derechos fundamentales de las personas.

A diferencia de otros datos, como una dirección o un número de teléfono, los biométricos no pueden ser cambiados fácilmente en caso de una vulneración de seguridad. Una vez que se filtra una huella dactilar o un patrón facial, es prácticamente imposible revertir el daño.

² Ley 25.326 art 2 tercer párrafo “Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.”

La doctrina jurídica³ suele considerar a los datos biométricos dentro de la categoría de datos sensibles debido al carácter único e irremplazables de los mismos. La biometría identifica a una persona de manera singular y permanente, lo que aumenta el riesgo de vigilancia indebida o discriminación.

Por otra parte, estos datos están vinculados a la esencia física de una persona, lo que convierte cualquier acceso no autorizado en una violación profunda a la privacidad individual.

Asimismo, la biometría es utilizada no solo para autenticación sino también para rastreo y monitoreo, lo que genera preocupaciones sobre el uso desmedido de la vigilancia.

Entendemos que los datos biométricos han adquirido una relevancia fundamental en la era digital, al punto de ser reconocidos como parte integral de los derechos humanos. El derecho a la protección de los datos personales está estrechamente vinculado al derecho a la privacidad, que es un derecho humano reconocido internacionalmente en diversos instrumentos legales. La creciente capacidad de las empresas, gobiernos y otras entidades para recolectar, procesar y almacenar datos de los individuos ha llevado a que la protección de los mismos sea una prioridad en las discusiones sobre derechos fundamentales. Dado que esta información refleja aspectos íntimos y únicos de la identidad de una persona, su protección es esencial para garantizar la dignidad y los derechos fundamentales.

El derecho a la privacidad está consagrado en la Declaración Universal de los Derechos Humanos⁴ y en el Pacto Internacional de Derechos Civiles y Políticos⁵. La protección de los datos personales es un componente esencial del derecho a la privacidad. Cuando la información personal es recolectada, almacenada o utilizada sin el consentimiento adecuado, se pone en riesgo la privacidad del individuo y, por extensión, su libertad y autonomía.

IV- Marco Normativo en Argentina

Argentina cuenta con una legislación robusta en materia de protección de datos. La Ley N.º 25.326 de Protección de Datos Personales establece principios fundamentales para el

⁴ Declaración Universal de los Derechos Humanos ART 12 “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”

⁵ Pacto Internacional de Derechos Civiles y Políticos ART 17 “1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.”

tratamiento de datos personales, la ley 26.388 ley de delitos informáticos, así como también el decreto 1766/11 los cuales son las bases para la regulación de datos personales en nuestro país, pero la regulación específica sobre datos biométricos es limitada,

Ley de Protección de Datos Personales (Ley 25.326)

La vigente Ley 25.326 fue sancionada en octubre del año 2000, y Publicada en el Boletín oficial el 2 noviembre del año 2000, fue pionera en su momento, esta ley establece un marco para la protección de datos personales, regulando la recolección, almacenamiento y uso de datos, incluidos los datos biométricos. Establece derechos para los titulares de los datos, como el derecho a la información, el acceso y la rectificación.

Esta ley establece definiciones amplias lo que permite encuadrar a los datos biométricos dentro de los datos sensibles, lo que implica un tratamiento más riguroso y la necesidad de consentimiento explícito para su uso.

Ley de Delitos Informáticos (Ley 26.388)

Esta ley incluye disposiciones relacionadas con la protección de datos en el ámbito de delitos informáticos, estableciendo sanciones para el acceso y uso indebido de datos personales.

Esta norma incorpora el artículo 153 bis al Código Penal el cual reza: *“Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.*

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.”

Decreto del Poder Ejecutivo Nacional Argentino N°1766/11

Este decreto crea el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS), este sistema tiene como objetivo central ser el marco para que la utilización de sistemas biométricos contribuyan a la seguridad pública y al esclarecimiento de hechos delictivos.

En primer lugar, el objetivo de este es lograr que todas las fuerzas de seguridad, tanto federales como provinciales, procesen rastros levantados de la escena del hecho sobre el SIBIOS y por otro lado, la identificación fehaciente de personas.

Fue necesaria la implementación de este sistema dado que se observó que las personas se trasladan, y cometen delitos en distintas jurisdicciones, por lo que el acceso a una base de datos común constituye un avance importante en materia de investigación criminal.

Código Civil y Comercial

El derecho a la privacidad está reconocido en el Código Civil y Comercial de la Nación en el artículo 52⁶, que establece que las personas pueden reclamar la reparación de los daños que sufran en su intimidad personal o familiar, honra, reputación, imagen o identidad.

El derecho a la privacidad protege la autonomía individual de una persona, que incluye sus sentimientos, hábitos, costumbres, relaciones familiares, situación económica, creencias religiosas, salud mental y física.

La intromisión en la vida privada de una persona solo puede justificarse por ley, cuando medie un interés superior que resguarde la libertad de los demás, la defensa de la sociedad, las buenas costumbres o la persecución del crimen.

Por otra parte, el artículo 53⁷ del Código Civil y Comercial de la Nación Argentina regula el derecho a la imagen y establece la prohibición de captar o reproducir la imagen o la voz de una persona sin su consentimiento.

V- Derecho comparado

⁶ Código Civil y Comercial Artículo 52.- Afectaciones a la dignidad. La persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos, conforme a lo dispuesto en el Libro Tercero, Título V, Capítulo 1.

⁷ Código Civil y Comercial artículo 53: "Derecho a la imagen. Para captar o reproducir la imagen o la voz de una persona, de cualquier modo que se haga, es necesario su consentimiento, excepto en los siguientes casos:

- a. Que la persona participe en actos públicos;
- b. Que exista un interés científico, cultural o educacional prioritario, y se tomen las precauciones suficientes para evitar un daño innecesario;
- c. Que se trate del ejercicio regular del derecho de informar sobre acontecimientos de interés general.

En caso de personas fallecidas pueden prestar el consentimiento sus herederos o el designado por el causante en una disposición de última voluntad. Si hay desacuerdo entre herederos de un mismo grado, resuelve el juez. Pasados VEINTE (20) años desde la muerte, la reproducción no ofensiva es libre".

Reglamento General de Protección de Datos (RGPD):

Fue sancionada en el año 2016, sin embargo, no fue hasta el 2018 que entró en vigencia. Aunque es una normativa de la Unión Europea⁸, su influencia ha llevado a la reflexión sobre la necesidad de una normativa más estricta en Argentina.

Este reglamento dispone que se requiere el consentimiento expreso para el procesamiento de datos, también establece derechos para los usuarios, como el derecho al acceso, rectificación y eliminación de datos.

Lo novedoso es que impone sanciones severas por incumplimiento (hasta el 4% de la facturación global de una empresa).⁹

Convenio N° 108 Del Consejo De Europa

Fue adoptado el 28 de enero de 1981 y es el primer tratado internacional vinculante sobre la protección de datos, para la Protección De Las Personas Con Respecto Al Tratamiento Automatizado De Datos De Carácter Personal, el cual garantiza a las personas el respeto a su vida privada en lo que respecta al tratamiento automatizado de sus datos personales.

VI- Uso de Datos Biométricos en Argentina

La aparición de estas nuevas tecnologías dio lugar a que en nuestro país se comiencen a utilizar los datos biométricos en diversas áreas.

La implementación de sistemas de reconocimiento facial en espacios públicos ha generado un debate sobre la seguridad versus la privacidad dado que en diversas plataformas utilizadas por organismos públicos los utilizan para reconocer personas. Incluso los registros civiles, sistemas de salud y hasta programas gubernamentales, lo están implementando para asegurar la identidad de los ciudadanos administrados.

⁸ **REGLAMENTO (UE) 2016/679 ART 1** “establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos”

⁹ **REGLAMENTO (UE) 2016/679 ART 83, 6:** El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Asimismo, los bancos, las financieras y muchas instituciones privadas utilizan datos biométricos para autenticar a los usuarios, lo que plantea interrogantes sobre la gestión y almacenamiento de estos datos. La mayoría de los bancos emplean tecnología biométrica para comprobar la identidad de sus clientes. Muchos requieren una toma de huellas digitales al abrir una nueva cuenta. Así, los bancos podrán verificar tu identidad fácilmente cuando visites una sucursal para hacer algún trámite. De igual manera, se utiliza tecnología de reconocimiento de voz para validar la identidad de sus cuentahabientes al comunicarse al centro de atención a clientes por teléfono.

Es por esto, que es necesario un control al acceso de las empresas y organizaciones que utilizan esos sistemas de reconocimiento, ya sea facial, huellas dactilares y escaneo de iris para evitar el uso indebido o divagación de estos datos.

VII- Desafíos en la Protección de Datos Biométricos

Los desafíos en la protección de datos biométricos son numerosos y complejos, especialmente en un contexto donde la tecnología avanza rápidamente.

Uno de los principales desafíos es el de obtener el consentimiento informado de las personas para la recopilación y uso de sus datos biométricos dado que las personas muchas veces no comprenden totalmente cómo se usarán sus datos o no tienen opciones para negarse y poder darle transparencia a la recopilación de los mismos.

Por otra parte, no todas las personas tienen el mismo acceso a la tecnología, lo que puede llevar a una desigualdad en la protección de datos. Las comunidades vulnerables pueden estar más expuestas a riesgos sin recibir la misma atención en términos de protección.

Es por esto que, la falta de conocimiento sobre la protección de datos biométricos entre la población puede resultar en una menor demanda de medidas de protección adecuadas y un mayor riesgo de abuso.

Por otra parte, los sistemas que almacenan los datos biométricos están constantemente expuestos a ciberataques dado que los cibercriminales están al acecho de estos. Lo que se busca es conseguir estos datos sensibles como las huellas dactilares o imágenes faciales, para el uso malicioso de los mismos. Esto trae consecuencias muy graves dado que los datos biométricos a diferencia de las contraseñas no pueden ser cambiados.

En muchos países, incluida Argentina, la legislación sobre protección de datos biométricos puede ser insuficiente o inexistente, lo que dificulta la regulación y el control del uso de estos datos frente a los avances tecnológicos. Es por esto por lo que, las autoridades no cuentan con los mecanismos necesarios y las empresas encuentran la forma de evadir las normas vigentes de privacidad, dado que la falta de estándares técnicos comunes puede dificultar la integración y el intercambio seguro de datos biométricos entre diferentes sistemas y entidades.

La implementación de tecnologías biométricas en contextos de seguridad pública puede dar lugar a la vigilancia masiva y el uso indebido de datos, lo que plantea preocupaciones sobre la privacidad y los derechos humanos.

Asimismo, la implementación de sistemas de seguridad para proteger datos biométricos puede ser costosa y técnica, y muchas organizaciones pueden carecer de los recursos o la experiencia necesarios. Y a medida que la tecnología avanza, los métodos de recopilación y análisis de datos biométricos evolucionan rápidamente. Esto puede dificultar la creación de regulaciones que se mantengan al día con las tendencias tecnológicas.

Abordar estos desafíos requerirá un enfoque coordinado que involucre a gobiernos, empresas, organizaciones de derechos humanos y la sociedad civil para garantizar una protección efectiva de los datos biométricos y el respeto por los derechos de las personas.

VIII- Estafas con utilización de datos biométricos:

Las estafas que involucran datos biométricos han ido en aumento debido a la creciente dependencia de estas tecnologías para la autenticación y la seguridad, estas estafas pueden realizarse mediante diferentes mecanismos.

Uno de estos mecanismos es la suplantación de identidad, esta consiste en que los delincuentes utilizan los datos biométricos robados, como huellas dactilares o reconocimiento facial, para poder acceder a cuentas y dispositivos personales. Esto puede incluir el uso de técnicas avanzadas para crear moldes de huellas dactilares o fotos de alta calidad para engañar a los sistemas de autenticación.

Por otra parte, también está el phishing de datos biométricos, eso se realiza mediante correos electrónicos o sitios web falsos, así como también por teléfono solicitando datos personales, en esta modalidad los estafadores pueden intentar engañar a las personas para que

proporcionen sus datos biométricos, afirmando que son necesarios para actualizaciones de seguridad o verificación de identidad. En algunos casos, los hackers pueden interceptar la transmisión de datos biométricos, especialmente si no se utilizan conexiones seguras. Esto puede suceder en entornos públicos o a través de redes Wi-Fi no seguras o utilizar algunos programas maliciosos diseñados para robar datos biométricos de dispositivos que los utilizan, como smartphones o computadoras. Estos pueden capturar información durante el proceso de autenticación.

Es por estas razones que es necesario para los usuarios utilizar autenticación de múltiples factores, mantener tus dispositivos actualizados y utilizar software de seguridad, y sobre todo, tener cuidado con los correos electrónicos y enlaces sospechosos.

IX- CONCLUSIONES

I. De lege lata:

La protección de datos biométricos en Argentina es un tema crucial que requiere atención inmediata. Con el avance de la tecnología y la creciente utilización de estos datos, es imperativo desarrollar un marco normativo adecuado, desarrollando regulaciones específicas para el uso de estos, asegurando límites claros para su utilización y de esta forma garantizar la protección del derecho a la privacidad de los ciudadanos. Es un desafío que involucra a todos: gobiernos, empresas y sociedad civil.

II. De lege ferenda:

Como explicamos anteriormente, entendemos que es fundamental establecer un marco legal claro y específico que regule el uso de datos biométricos, considerando su naturaleza sensible.

Esto incluiría directrices sobre la recolección, almacenamiento, procesamiento y eliminación de estos datos.

Argentina podría fortalecer su marco legal adoptando algunas de las disposiciones del Reglamento General de Protección de Datos (RGPD), como aumentar las sanciones, mejorar el control sobre el consentimiento, y garantizar una notificación rápida de violaciones de seguridad, poder acceder al derecho al olvido, donde los usuarios tengan derecho a solicitar la eliminación de sus datos personales cuando ya no sean necesarios para los fines originales, medidas que ayudarían a prevenir abusos en el manejo de datos sensibles.

Por otra parte, es necesario el fortalecimiento de la autoridad de protección de datos, es decir aumentar los recursos y capacidades de la Agencia de Acceso a la Información Pública para que puedan supervisar efectivamente el uso de los datos biométricos, garantizar el cumplimiento de la legislación y aumentar las sanciones para empresas que no cumplan con la ley, poniendo en marcha mecanismos más claros de supervisión.

Es necesario asimismo, crear canales accesibles para que los ciudadanos puedan denunciar abusos o infracciones relacionadas con el uso de sus biométricos.

Y por último, promover la educación y concientización, creando programas de capacitación y educación desde los organismos públicos y las empresas, así como también en los distintos niveles educativos, para poder crear una cultura de la protección de datos en todos los niveles.