Departamento de Ciencias Jurídicas
Universidad de Atacama, Chile
ISSN 2735-6507

POSIBLES RIESGOS Y PROBLEMAS DEL USO DE DATOS BIOMÉTRICO Y SU RELACIÓN CON LOS DERECHOS FUNDAMENTALES.

Khalil Franco Ceratto[1]
Johan Paul Veloz Quezada[2].

Resumen

La presente investigación mediante el método de análisis cualitativo, análisis histórico-jurídico y el método de análisis jurídico-comparativo, buscara estudiar el uso de los datos biométricos, identificando los riesgos que presenta la implementación de este tipo de tecnología con los Derechos Humanos. Al igual que otros sistemas utilizados para el control social, la biometría plantea potenciales vulneraciones a los derechos de libertad de expresión, asociación e información, por lo cual, también es pertinente analizar las formas en que se relacionan los datos y las tecnologías biométricas con los Derechos Humanos de las personas, con el fin de poder identificar las desventajas de estos sistemas tecnológicos en relación a la vulneración de los derecho establecidos en los Tratados y Convenios Internacionales.

Palabras clases: Datos biométricos, derechos, estado, igualdad, grupos de poder.

Introducción

La primera parte de este artículo de investigación se encargará de analizar a profundidad la conceptualización de la Biometría y los Datos Biométricos, estableciendo cual es la naturaleza jurídica de estos, además de sus características y funciones, para que, a partir de esas bases, se pueda analizar la

[1] Email: khalilfrancoceratto2000@hotmail.com
Orcid: https://orcid.org/0000-0003-3761-4914
Universidad Metropolitana del Ecuador

[2] Email: gohangaymer020@gmail.com
Orcid: https://orcid.org/0000-0001-5927-6157
Universidad Metropolitana del Ecuador

colisión que se da entre la aplicación de la Biometría y su relación con los Derechos Fundamentales de las personas, a partir de las desventajas que se presentan en el mundo jurídico.

Según la Comisión IDH (2017) en su Relatoría Especial para la Libertad de Expresión estableció que:

> 203. El funcionamiento de internet depende de la creación, almacenamiento y administración de datos personales y de otro tipo. Ello implica que una enorme cantidad de información sobre las personas pueda ser interceptada, almacenada y analizada por los Estados y por terceros.

Es decir, actualmente nos encontramos en un mundo globalizado, donde el intercambio y flujo de información se da a escala global, ya que el desarrollo de las sociedades está ligado con la información, la misma que está dirigida por la globalización. En este contexto nos encontramos con una era informática. Frente a esta realidad tan cambiante y los imparables avances tecnológicos que se dan día a día, los diversos sistemas jurídicos del mundo han tratado de ir adoptando y reconociendo progresivamente el derecho a la privacidad y seguridad de nuestros datos personales, de acuerdo con las necesidades que presenta el mundo moderno.

Estos avances progresivos de los derechos y las legislaciones de varios países en Latinoamérica y el mundo han reconocido que los datos personales de los individuos deben ser protegidos en concordancia con el derecho fundamental a la privacidad y que por lo tanto cada persona tiene hasta cierto punto un grado de control sobre esta información. Conforme a esta facultad, el titular de los datos debe ser capaz de controlarlos, compartirlos y excluirlos de la vida pública, conforme a su voluntad.

Dentro de aquellos datos personales que deben ser protegidos, existe una subcategoría llamada datos sensibles, los cuales comúnmente se

refiere a todos aquellos datos que se relacionan con el nivel más personal de su titular, conformada por antecedentes relativos a la persona y que por sus características e importancia, su divulgación pueda ser causa de vulneración de distintos Derechos Fundamentales.

Los datos biométricos debido a su naturaleza caben dentro de esta categoría, ya que han trascendido en el mundo moderno como una poderosa herramienta para identificar, verificar y almacenar los datos de sensibles de millones de individuos en diversos sistemas informáticos.

Si bien la biometría es un tipo de tecnología que trae muchos beneficios para la ejecución de muchas actividades que van desde algo tan básico como comprar en el supermercado hasta espionaje internacional, su uso cada vez es más frecuente alrededor del mundo y puede ser sumamente beneficiosa para la optimización y la eficiencia de diversos procesos de la vida en sociedad, pero también representa un enorme riesgo para los individuos, ya que si se utiliza de manera irresponsable y sin ningún tipo de regulación es posible que resulten vulnerados derechos fundamentales consagrados tanto a nivel local como a través de tratados internacionales.

En el siglo XXI la implementación de datos biométricos por parte de las personas se da cotidianamente, a veces, sin el consentimiento de algunas personas. Se puede aplicar hasta en el simple uso de nuestro dispositivo móvil con reconocimiento de huellas o de reconocimiento facial. Es decir, la huella de los dedos, el rostro, la forma de moverse, son características biométricas únicas en cada persona, que a partir de la tecnología biométrica se puede utilizar para ejecutar todo tipo de procesos rutinarios de una manera más segura, rápida y eficaz.

La biometría tiene muchas más ventajas frente a otros sistemas de autenticación como el uso de tarjetas,

contraseñas o pulseras, ya que es más cómodo, no se puede perder u olvidar, no tiene un gasto de mantenimiento, no necesita renovación y sobre todo, es muy difícil de falsificar, por lo que es totalmente segura. Pero al llegar a ser tan personal, necesita de una manipulación y control de mucho cuidado.

Es por esto que esta investigación mediante el método de análisis cualitativo, análisis histórico-jurídico y el método de análisis jurídico-comparativo buscará identificar las relaciones y los conflictos que se presentan entre el uso de los datos biométricos y los Derechos Humanos de las personas. Partiendo de esto, indagaremos los riesgos que representa la implementación de tecnologías biométricas en las sociedades donde no hay un contexto jurídico adecuado, además de los obstáculos que el derecho debe sortear para para poder lograr una armonía que proteja nuestros Derechos Fundamentales, pero al mismo tiempo nos permita gozar de ellos libremente pero con una mayor protección.

DESARROLLO

CONCEPTO DE BIOMETRÍA:

Etimológicamente la palabra "biometría" tiene su origen en las palabras: *bio*, que significa vida, y *metron* que significa medida. Así, es como la biometría vendría a ser la medida de mi vida o de la vida.

La biométrica científicamente, tiene amplias descripciones, pero en general, se basa en la identificación de los rasgos únicos de cada persona que permite diferenciarla de los demás. Para Serratosa (2008) "La biometría es una ciencia que analiza las distancias y posiciones entre las partes del cuerpo para poder identificar o clasificar a las personas".

Es decir, en cada persona, existe un sinfín de datos, caracteres y rasgos únicos e irrepetibles que la hacen sobresalir de los demás. Tal cual advierte Olivares (2009)

> La biometría está basada en el principio de que cada individuo es único y posee rasgos físicos distintivos (rostro, huellas digitales, iris de los ojos, etc) o de comportamientos (la voz, la manera de firmar, etc.), los cuales pueden ser utilizados para identificarla o validar restricciones de acceso. (p.29)

DATOS BIOMÉTRICOS:

Si la biometría, se encargaba de analizar los rasgos físicos y de comportamiento en una persona para diferenciarla de las demás. Sin caer en redundancia, los datos biométricos vendrían a ser el conjunto o la totalidad de todos estos datos, con un orden establecido y para un fin determinado.

Para la Comisión IDH (2017) en su Relatoría Especial para la Libertad de Expresión, los datos biométricos son aquellos:

> 209. Que permiten "el reconocimiento sistemático de individuos basado en sus características conductuales y biológicas". El mecanismo de uso de datos biométricos supone la recolección de datos biológicos, como las huellas digitales, el iris, el ADN, la voz, etc. y la sistematización de todos esos datos en una única base de datos, que, combinada con otras fuentes de información conductual, permiten, bajo un sistema de probabilidad, identificar a las personas.

Según Sánches & Rojas (2018):

> Por definición común, los datos biométricos son aquellos rasgos físicos, biológicos o de comportamiento de un individuo que lo identifican como único del resto de la población, como: huellas dactilares, geometría de la mano, análisis del iris, análisis de retina, venas del dorso de la mano, rasgos faciales, patrón de voz, firma manuscrita, dinámica

del tecleo, cadencia del paso al caminar, análisis gestual y análisis de ADN. (p.2)

Ya en contexto, podemos darnos cuenta que, el término "datos biométricos" es muy general, pues dentro de estos, no solo encontramos un tipo en específico de información, sino de distinta naturaleza. En relación a lo anterior, Muñoz (2017) los clasifica en dos grandes categorías:

Datos Biométricos Estáticos:

Son aquellos datos que se relacionan en mayor medida con características físicas o estructurales de las personas y que, por lo tanto, son en general permanentes en el tiempo, ya que se relacionan directamente con órganos o sistemas anatómicos humanos. Dentro de este tipo de datos se encuentran los datos respecto al ADN, las huellas dactilares, el color del iris, los rasgos faciales, la piel o la composición química del cuerpo. (p.3)

Datos Biométricos Dinámicos:

En contraposición a las formas estáticas, los datos biométricos dinámicos se determinan en relación con características funcionales o del comportamiento de las personas. Este comportamiento se diferencia profundamente de los datos estáticos, ya que debido a su naturaleza no sólo tiene aptitud para mutar, sino que es muy probable que ocurra durante la vida del individuo. Dentro de este tipo de datos encontramos información relativa a la forma de caminar, el comportamiento al firmar, el ritmo al hablar, forma de teclear, o gestos y movimientos corporales. (p.12)

CARACTERÍSTICAS: AHONDAR EN CARACTERISTICAS

Cuando hablamos de datos biométricos, sin duda, hay características

o factores que los hacen muy especiales. Pero esta singularidad, definitivamente está ligada al sentido personalísimo que tiene la biometría y los datos biométricos recogidos en cada persona. Datos que como sabemos son únicos e irrepetibles.

Según Garrido Iglesias & Becker Castellaro (2017) los datos biometricos tienen dos caracteristicas fundamentales:

- Son obtenidos por tratamientos automatizados para verificar o determinar la identidad de personas a través de características fisiológicas o conductuales
- Reconocen características fisiológicas, físicas, conductuales o psicológicas: las características fisiológicas o físicas se definen como medidas o mediciones a parte o partes del cuerpo humano (escáner al iris o huellas dactilares, patrones geométricos del rostro u orejas, reconocimiento de voz, etcétera). Por su parte, las características conductuales o psicológicas se basan en acciones derivadas directa o indirectamente de las características del cuerpo humano. (pag.69)

De igual manera Korja (2006) afirma que para que los datos biométricos puedan cumplir la función de identificar a las personas, o bien autentificarlas, deben cumplir con las siguientes características:

• Medibles: la facilidad por la cual es posible leer el dato.

• Robustos: en cuanto a cómo el dato individual va modificándose con el tiempo.

• Aceptables: deben mostrar aspectos positivos del individuo.

• Universales: que toda población tenga aquel dato que se extrae del individuo.

• Distintivos: debe mostrar una gran variabilidad sobre el resto de la población para asegurar la individualidad del dato en cuestión. (pag.69)

Departamento de Ciencias Jurídicas
Universidad de Atacama, Chile
ISSN 2735-6507

A partir de lo establecido previamente podemos inferir que las características de los datos biométricas pasan por los siguientes ejes principales:

Perpetuidad de datos biométricos: la información biométrica posee una relación esencialmente intrínseca con una única persona de la cual proviene la información.

Mismo dato en diferentes sistemas: debido a que los datos biométricos son propios de una persona y perpetuos, el usuario utiliza los mismos datos en diferentes sistemas.

Requisito de acción por parte del titular: los sistemas de datos biométricos ofrecen la posibilidad de que el usuario nunca llegue a enterarse que su información está siendo utilizada. Es común que se obtenga, por lo tanto, a través de objetos, rastros, o cámaras de vigilancia.

FUNCIONES:

Con relación a las funciones de la tecnología biométrica, mencionamos las siguientes:

Identificación:

Según la ONU (2018) esta función también es conocida como:

> "*comparación uno de muchos o 1: n,* esto es debido a que "no se depende de una identidad sugerida y por lo tanto la plantilla de consulta interroga a toda la base de datos para obtener una posible coincidencia. El software de búsqueda y combinación arroja un puntaje de similitud para posibles coincidencias y selecciona en forma automática una coincidencia de alta confianza o presenta una lista de candidatos de coincidencias sugeridas a un operador humano para su comparación con la plantilla de consulta". (pag.13).

Verificación:

Departamento de Ciencias Jurídicas
Universidad de Atacama, Chile
ISSN 2735-6507

Esta función dentro de las tecnologías biométricas tiene un papel trascendental ya que como afirma Muñoz (2017) su proceso corresponde a:

> Comprobar que la identidad de un individuo coincide o corresponde con la que este señala ser. La verificación es un proceso de confirmación de identidad, no una búsqueda, y a diferencia del proceso de identificación, se realiza haciendo una comparación uno a uno, es decir la muestra se contrapone con el dato específico de esa persona en la base de datos, no es una comparación general. (p.15)

Asimismo, la ONU (2018) menciona que "la verificación es conocida también como un proceso de comparación uno a uno o 1:1". Es decir, la verificación permite demostrar si eres la misma persona cuya identidad ya ha sido autenticada y registrada en una base de datos.

A partir de lo esgrimido en esta sección, es importante hacer notar que tanto la función de identificación como de verificación forman parte de un proceso de reconocimiento, es decir constatar y comparar información con datos previamente ingresados, con el fin de poder identificarte e individualizarte dentro de una base de datos.

NATURALEZA JURÍDICA DE LOS DATOS BIOMÉTRICOS:

Para comenzar el establecimiento de la naturaleza jurídica es necesario preguntarnos ¿Somos nuestros cuerpos, o son nuestros cuerpos parte de nosotros? Esto significa que, cuando nos referimos a los datos biométricos tradicionalmente, nos hacemos la idea de reconocer al dato biométrico como parte del ámbito de la protección de nuestra intimidad y privacidad, hablar de esto conlleva a la regularización por parte de un marco normativo de protección de datos

personales que muchas veces no existe o no está bien definido.

Es así que, cuando se trata de datos personales que se encuentran dentro del espectro informático tan cambiante, infinito y con numerosos desafíos tanto para el Estado, en su rol de garante, como para los particulares, en su rol de usuarios, ningún marco normativo en el mundo es suficiente para asegurar la protección de los datos biométricos de cada integrante de la sociedad.

Por lo anterior, la Comisión IDH (2017) en su Relatoría Especial para la Libertad de Expresión estableció que:

> 194. Los Estados tienen la obligación de respetar y proteger el derecho a la privacidad en la era digital y adoptar o adaptar su legislación y sus prácticas al efecto, protegiendo a todas las personas bajo su jurisdicción –incluyendo conforme al derecho internacional, aquellas personas sobre las cuales tenga control efectivo- sin discriminación por origen nacional, nacionalidad, sexo, raza, religión o cualquier otro motivo.

En relación a lo anterior, Muñoz (2017) menciona que el concepto de dato personal conlleva implícito dos ideas, en primer lugar, la idea del dato, que es “información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho”. Por otro lado, se encuentra el carácter de personal, en virtud del cual debe existe una “conexión de este dato con una persona identificada o identificable”. En caso de no existir tal relación, la información contenida en esos datos será anónima y por lo tanto no será merecedora de protección por parte de ordenamiento jurídico”.

Es decir, la naturaleza jurídica de los datos biométricos pasa por una de sus principales funciones, que es identificar a un individuo acorde a ciertas cualidades y características intrínsecas a el que permite diferenciarlo de los demás.

Departamento de Ciencias Jurídicas
Universidad de Atacama, Chile
ISSN 2735-6507

Por lo mencionado en párrafos precedentes, podemos observar como empieza a surgir la necesidad de que exista un marco normativo integral para la aplicación de los datos biométricos, que permita el disfrute de estas herramientas pero al mismo tiempo que establezca limites a su uso de acuerdo contexto social en donde se desarrolle y siempre a favor de la protección de los Derechos Humanos de las personas.

DATOS BIOMÉTRICOS Y SU RELACIÓN CON LOS DERECHOS HUMANOS.

Divulgación no autorizada

Para una mejor comprensión de esta sección de la investigación relacionaremos la divulgación no autorizada de los datos biométricos con el derecho a la propiedad.

Doctrinariamente el derecho a la propiedad está muy bien sustentado y completo, este derecho, hace referencia al derecho que las personas tienen sobre aquellas cosas incorporales que se encuentran relacionadas a su personalidad, como su nombre, su imagen y su voz, por lo tanto pueden ejercer control y dominio sobre su información personal, precisamente porque refieren que los datos personales son parte de su patrimonio, es decir se puede impedir que recepten, almacenen o utilicen de forma arbitraria sin ningún tipo de consentimiento.

Lo anterior se relaciona con el derecho de las personas de poder elegir el destino y utilización de sus datos, en cuanto a lo que establece el Tribunal Constitucional Alemán:

> El derecho a la protección de datos ha de enmarcarse en el derecho general de protección de la personas, por considerar que garantiza la facultad del individuo a determinar por sí mismo la divulgación y utilización de datos referentes a su persona.

De lo mencionado previamente, se establece que la privacidad de los datos personales está ligada a la

Departamento de Ciencias Jurídicas
Universidad de Atacama, Chile
ISSN 2735-6507

titularidad de derecho que tiene cada persona en relación a sus datos biométricos, en la cual se establece como principio fundamental el consentimiento expreso y voluntario de las personas para la utilización de sus datos biométricos y todo uso de estos sin previa autorización será una transgresión arbitraria a su derecho a la propiedad, puesto que cada persona dentro de la sociedad tiene derecho a tener el control de sus datos personas.

Por otro lado, aparece también, la doctrinariamente llamada "auto terminación informativa" ya que debemos entender que el uso de tecnologías y la recolección de datos biométricos, no va afectar a un único derecho, sino que podría transgredir la información en todas las esferas de la vida de una persona.

Para solucionar este conflicto, en cierta parte, ponderativo, hay que contextualizar la situación, ya que debido a la globalización la protección de datos personales no solo tienen que ver con nuestra privacidad, sino que hay que tener en consideración la evolución tecnológica e informática que facilita la interacción de esos datos, su tratamiento, su transferencia, y que en definitiva facilita mucha la vida, pero siempre deben ir de la mano con un marco normativo que pueda estar presente siempre vigilando cualquier trasgresión.

Ya que según Muñoz (2017) lo importante es "la capacidad que tiene el titular de los datos para elegir con quién y de qué forma compartir su información personal, y especialmente su información personal sensible".

Vigilancia, rastreo y contante observación

Para poder tener una mayor comprensión de la magnitud de los problemas que se presentan a partir del uso de la vigilancia y rastreo sin un marco jurídico adecuado que proteja los derechos fundamentales de las personas, es necesario citar casos estableciendo por la Comisión Interamericana:

Departamento de Ciencias Jurídicas
Universidad de Atacama, Chile
ISSN 2735-6507

a) Fallo Escher y Otros vs. Brasil

A breves rasgos este caso se enmarca en las distintas políticas públicas que permiten a las empresas de telecomunicaciones y otros proveedores de servicios de Internet a capturar y conservar de manera indiscriminada los datos de registro o metadatos generados sobre las comunicaciones y actividades en línea de sus usuarios, permitiendo a las autoridades encargadas de hacer cumplir la ley, acceder posteriormente a estos datos en sus tareas de seguridad, investigación y persecución del delito.

En este caso en particular la Corte IDH desarrollo de manera muy completa el derecho a la privacidad estableciendo lo siguiente:

> La protección del derecho a la privacidad comprende tanto las operaciones técnicas dirigidas a registrar el contenido de las comunicaciones, mediante su grabación y escucha, "como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones
>
> En su Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión, esta Oficina reconoció de manera particular que los metadatos de las comunicaciones digitales, que incluyen, entre otros, la ubicación, actividades en línea, y con quiénes se comunican los usuarios de Internet, pueden ser altamente reveladores, y su recolección y conservación equivalen a una limitación directa al derecho a la intimidad y vida privada de las

personas. En el reciente informe El derecho a la privacidad en la era digital, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos indicó que desde el punto de vista del derecho a la privacidad, "[l]a agregación de la información comúnmente conocida como 'metadatos' puede incluso dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada".

En su informe sobre las consecuencias de la vigilancia de las comunicaciones por los Estados en el ejercicio de los derechos humanos a la intimidad y a la libertad de opinión y expresión, el Relator Especial de las Naciones Unidas (ONU) para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, Frank La Rue, indicó que "la conservación obligatoria de datos está facilitando la recopilación a gran escala de datos que luego pueden refinarse y analizarse". El Relator afirmó que estas políticas "son invasivas y costosas, y atentan contra los derechos a la intimidad y la libre expresión. Al obligar a los proveedores de servicios de comunicaciones a generar grandes bases de datos acerca de quién se comunica con quién telefónicamente o por Internet, la duración del intercambio y la ubicación de los usuarios, y a guardar esta información (a veces durante varios años), las leyes de conservación obligatoria de datos aumentan considerablemente el alcance de la vigilancia del Estado, y de este modo el alcance de las violaciones de los derechos

humanos. Las bases de datos de comunicaciones se vuelven vulnerables al robo, el fraude y la revelación accidental". En este informe, el Relator recomendó a los Estados no exigir la retención de información determinada puramente con fines de vigilancia.

b) Malware "Pegasus"

Entre enero de 2015 y agosto de 2016 en la Ciudad de México se dio un espionaje masivo a diversos periodistas y defensores de los derechos humanos a través de un virus informático que afectaba al teléfono inteligente, permitiendo el acceso a los archivos guardados en el equipo, así como a los contactos, mensajes, correos electrónicos. El malware también obtiene permisos para usar, sin que el objetivo lo sepa, el micrófono y la cámara del dispositivo.

c) Caso de Guatemala

En el año 2008, estalló con conflicto en el cual el Estado de Guatemala habría adquirido software y equipos técnicos que poseen la capacidad de interceptar teléfonos y redes sociales de personas influyentes dentro de la sociedad guatemalteca. Según información pública los equipos habrían sido adquiridos con fondos de la Dirección General de Inteligencia Civil (Digici) que depende orgánicamente del Ministerio de Gobernación. Además, desde la Digici se habría llevado a cabo los hechos de interceptación. Otros equipos habrían sido adquiridos con fondos de la Policía Nacional Civil (PNC) y también de la Secretaría de Inteligencia del Estado. Según la información disponible, se habrían adquirido equipos tecnológicos como Circles, y programas como Pegasus, Pen-Link, Laguna, Citer 360, entre otros, que poseen la capacidad de interceptar llamadas, desencriptar mensajes, extraer datos de llamadas, entre otras capacidades. Asimismo, para la adquisición de estos programas se habrían diseñado contratos en cuyas

Departamento de Ciencias Jurídicas
Universidad de Atacama, Chile
ISSN 2735-6507

especificaciones técnicas figurarían informaciones generales descriptas como "seguridad del Estado".

A partir del extracto de casos reales que se han presentado, podemos apreciar solo la punta del iceberg del gran problema que se presenta cuando se implementan este tipo de tecnologías, ya que sin duda todas estas prácticas no permitirían un libre desarrollo de la personalidad coartan muchos derechos que se interrelacionan entre sí, por lo anterior, es necesario un marco regulador que se acople a los estándares internacionales para que los Estados puedan garantizar que cada parte del proceso de recolección, procesamiento y uso de estos datos tan importantes no vulneren derechos fundamentales.

Disminución y negación del anonimato y su incidencia en la privacidad del comportamiento

Sin duda uno de los derechos menos desarrollados en Latinoamérica, el derecho al anonimato, es un eje central en cuanto al libre desarrollo de las personas, ya que tiene relación con la libertad de cada individuo de comportarse de acuerdo a su voluntad en un ambiente de extrema intimidad y confianza sin ser observado, ni cuestionado por nadie.

En cuanto a este derecho la Comisión IDH (2017) en su Relatoría Especial para la Libertad de Expresión, afirmo lo siguiente:

> La garantía de la privacidad y el anonimato también forman parte de los derechos de asociación y reunión. Sin perjuicio de lo cual, no ampara todo tipo de expresiones o asociaciones. Por el contrario, "el anonimato del emisor de ninguna manera protegería a quien difunda

Departamento de Ciencias Jurídicas
Universidad de Atacama, Chile
ISSN 2735-6507

> pornografía infantil, a quien hiciera propaganda a favor de la guerra o apología del odio que constituya incitación a la violencia o incitare pública y directamente al genocidio". Los Estados deben garantizar la plena protección del discurso anónimo y regular los casos y condiciones específicas cuando dicho anonimato deba ser levantado, requiriendo para ello control judicial suficiente y la plena vigencia del principio de proporcionalidad respecto de las medidas tendientes a identificar a la persona en cuestión.

Por otro lado, Garrido Iglesias & Becker Castellaro (2017) afirman que:

> El que existan varias fuentes con datos biométricos fluyendo en el mundo digital hace que disminuya paulatinamente el anonimato en espacios públicos y privados. Los datos biométricos son información que va esencialmente contra el anonimato, debido a la facilidad y exactitud con que pueden identificar, rastrear o distinguir a las personas. (pag.86)

Como es de conocimiento general a través de las redes sociales, se pueden rastrear a personas con reconocimiento biométrico para que puedan ser identificadas y etiquetadas en sus fotos. Es por esto, que cada vez es más fácil detectar e identificar por qué persona y bajo qué circunstancias, fue realizada cada acción. Pero lo peor sin duda no pasa aquí, sino, por la normalización de la sociedades del siglo XXI exponer datos personales e íntimos en internet, ya sea por páginas web o por las famosas redes sociales, sin antes consultar o estar al tanto de los grandes riesgos que esto implica para mi seguridad y para la de mis datos.

Para ejemplificar con más profundidad la afectación del derecho a la privacidad y todos los derechos

interrelacionados a ella, presento el siguiente ejemplo:

a) Sistema de Vigilancia Móvil en la Región Metropolitana de Santiago, Chile

Según el informe de la Oficina de Relatoría Especial para la libertad de expresión en 2019 fue presentado un nuevo Sistema de Vigilancia Móvil que mediante el uso de drones y cámaras de alta definición buscaría combatir la delincuencia y ayudar en la coordinación de las distintas autoridades regionales y comunales en el trabajo conjunto y eficiente para mejorar la seguridad mediante la obtención información visual y de reconocimiento facial automatizado para transmitirla en vivo a centrales de monitoreo ubicadas en las intendencias regionales, donde operadores capacitados observarían las imágenes que entregan los drones.

Es menester establecer que el uso de este tipo de tecnología biométrica en las sociedades es muy delicado, debido a que el constante monitoreo de las personas a través de su información, ubica a las personas en una situación de incomodidad al sentirse observadas o controladas a diario, trasgrediendo muchos derechos importantes para el libre desarrollo de su personalidad.

Discriminación

Para poder entender de manera integral la discriminación por parte del uso de tecnología biométrica, es necesario analizar su interrelación con su antónimo, el derecho a la igualdad. Garantizar este derecho en todas las esferas de la sociedad, es sin duda alguna una de los deberes y las aspiraciones más grandes de todos los estados e instituciones a nivel mundial, pero al mismo tiempo es uno de los derechos más difíciles de consolidar y de garantizar debido a la desigual estructuración de las sociedades en el mundo.

Internacionalmente el derecho a la igualdad está altamente reconocido. En la Declaración de los Derechos Humanos de las Naciones Unidas (1948)

el Artículo 21.1 dice que "toda persona tiene el derecho de acceso, en condiciones de igualdad, a las funciones públicas de su país".

Así mismo, la Convención Americana sobre los Derechos Humanos (1969) en su artículo 24 establece la igualdad ante la Ley, donde dice que "todas las personas son iguales ante la ley. En consecuencia, tienen derecho, sin discriminación, a igual protección de la ley". Después en su Artículo 23.1.c establece los Derechos Políticos, donde enmarca que todos los ciudadanos deben "[…] de tener acceso, en condiciones generales de igualdad, a las funciones públicas de su país".

La discriminación se puede relacionar a la biometría y al principio de igualdad, por ejemplo, en la esfera tanto pública como privada de los proveedores de bienes y servicios.

Dentro de la esfera privada, los datos biométricos pueden utilizarse para negar a una persona un determinado servicio o bien. Como muy bien lo explica Muñoz (2017) las empresas privadas "pueden utilizar este tipo de tecnología para identificar personas según su historial y por lo tanto quebrantar la presunción de inocencia presente en nuestro ordenamiento".

Es decir, tal vez sea más sencillo pagar mi comida, poniendo mi huella digital en un scanner, que permita el acceso limitado al dinero de mi cuenta bancaria, para poder pagar mi almuerzo, pero también podrían tener acceso a mi información de salud, mis finanzas personales y en este caso específico a mi historial delictivo, convirtiendo mis datos más íntimos e importantes en públicos. Todo esto, seguramente debido a los problemas estructurales que acechan a las sociedades desde siempre, podría desencadenar actos de discriminación, lo que estaría afectando directamente al derecho o principio de igualdad de las personas.

Otro caso, podría ser, que las tecnologías tan avanzadas funcionen correctamente en personas o sujetos

dentro de un estándar determinado o entre una determinada edad. Estudios afirman que los scanner dactilares no funcionan correctamente en niños ni en adultos mayores, podemos notar que claramente, que si lleva a cabo algún tipo de proceso de recolección de datos, para brindar un determinado servicio a la población y se lo realiza por este método, quedarían excluidos.

Dentro de la esfera pública, casi ocurre lo mismo, pero pueden llegar a ser mucho más perjudiciales, ya que el estado es el encargado de brindar servicios de calidad y gratuitos a todos sus habitantes, si el estado no te brinda y no te garantiza los derechos y servicios que como ciudadano te corresponden, nadie lo hará, tendrás que buscarlo por tus propios medios en la industria privada.

Es así, que Garrido Iglesias & Becker Castellano (2017) explica este riesgo nace "en virtud de que el poseer datos tan sensibles como la huella digital, rostro de las personas u otros permitiría generar discriminaciones arbitrarias a personas en la entrega de productos, servicios o en el otorgamiento de derechos por parte del Estado".

Siguiendo esta misma línea, Muñoz (2017) dice que:

> El Estado juega aquí también un papel importante, pues en virtud de las potestades que ostenta, tiene facilidades para exigir a los ciudadanos la entrega de ciertos datos, y el sometimiento a la toma de muestras para la obtención de la información, debiendo tomarse mayores precauciones en materia de discriminación.

Es decir, a partir de tus datos se generarán bancos de información en torno a los datos sensibles y más íntimos a las personas y se crearon procesos de selección automáticos de acuerdo a determinadas características previamente estudiadas sin si quiera tener un contacto previo con las personas.

Departamento de Ciencias Jurídicas
Universidad de Atacama, Chile
ISSN 2735-6507

Derecho de la integridad física y psíquica:

El derecho a la integridad personal engloba tanto la parte física, moral y psíquica. Dentro de la legislación internacional encontramos en el artículo 5.1 de la Convención Americana de Derechos Humanos (1969) los Derechos a la Integridad Personal donde dice que "toda persona tiene derecho a que se respete su integridad física, psíquica y moral".

Los datos biométricos en relación a la vulneración del derecho fundamental a la integridad, se puede dar de muchas maneras. La integridad física y su relación con los datos biométricos, se basa en la necesidad de exponer el cuerpo humano en la recolección de muestras.

Para recolectar estos datos, Muñoz (2017) establece que se da una "invasión física importante al requerir contacto o proximidad con el cuerpo, discusión que cobra una mayor relevancia aún, si consideramos que la toma de muestras en muchos casos puede significar radiación electromagnética, o el requerimiento de fluidos corporales".

Por otro lado, según Domaica, (2019) "se deduce así, unas características del derecho integridad física, que podemos enunciar como integridad equivalente a incolumidad corporal, o derecho a no sufrir lesión o menoscabo en el cuerpo sin consentimiento".

Siguiendo la misma línea argumentativa Díaz (2018) afirma que "Desde el momento mismo de su recolección, los datos biométricos pueden causar una serie de preocupaciones e incomodidades relacionadas con normas culturales, miedos y circunstancias contextuales y sociales". Para la autora

> En ciertas culturas o religiones, los procesos de recabar las huellas digitales o el iris del ojo pueden resultar invasivos, incómodos o humillantes; los niños y adultos mayores pueden

> sentir temor a las máquinas que deben entrar en contacto con sus cuerpos; las personas discapacitadas y LGBTQI pueden verse excluidas, afectadas o discriminadas a través del proceso de categorización y clasificación de sus cuerpos mediante parámetros de lo que se defina como "normal" Por otra parte, si bien la implementación a escala colectiva de tecnologías biométricas. (p.8)

La toma de datos biométricos, estos que, son tan intrínsecos de la persona, suponen un problema que puede generar todo tipo de debate alrededor del mundo y en muchas culturas por diversos motivos tales como religión, moral o espiritual. Ya que todo el proceso que engloba manejar los datos biométricos requiere un nivel de proximidad muy íntimo hacia las personas lo cual sin duda vulneraria todo el abanico de derechos relacionados a la intimidad y a la privacidad. Por otro lado, es necesario mencionar que actualmente también existen diferentes tipos de procedimientos en los cuales se extraen y almacenan los datos biométricos de las personas sin que estas se dan cuenta de lo que está pasando.

Conclusión

Hablar sobre los datos biométricos nos ha traído grandes dudas y sobre todo pensamientos innovadores que vendrían mejorar el futuro para la sociedad y el derecho, más que todo para la seguridad ya que con la debida aparición y el uso de los datos y la tecnología biométrica es solo un pequeño resultado, es solo la punta del iceberg, de lo que se nos aproxima como sociedad, es decir una total transformación globalizada influida por el desarrollo de tecnologías altamente eficientes que traerán consigo muchos cambios dentro de cómo nos comportamos dentro de la sociedad.

Los datos biométricos surgen dentro de este contexto, simplificando, mejorando y facilitando mecanismo de seguridad y de acceso a servicios, que ya han quedado obsoletos debido a sus procesos tan arcaicos.

De esta lógica surge entonces la siguiente conclusión: el uso de la tecnología biométrica puede traer grandes beneficios debido a que puede facilitar varias esferas de la vida en general, sin embargo, es importante que esta sea utilizada siempre en base a ciertos principios, con el fin de no solo vulnerar la privacidad sino además otros derechos fundamentales como la no discriminación arbitraria, lo que afecta el marco normativo que debiese tener un Estado de derecho democrático

Sin duda alguna, uno de los riesgos más grandes que hay que tener presente según Garrido Iglesias & Becker Castellaro (2017) son "la falibilidad de los sistemas biométricos por la naturaleza de los datos (públicos, únicos, muy difíciles de reemplazar), y el otro es sus usos o tratamiento" ya que sin duda alguna, las inmensas bases de datos que cuentan los Estados o las transnacionales son una mina de oro para la discriminación en el otorgamiento de servicios o derechos por parte de empresas o entidades estatales que poseen y analizan datos biométricos, generar identidades falsas, divulgación no autorizada, etc.

Terminando con nuestra investigación, sería muy pertinente reflexionar y preguntarnos o más pertinente seria aun, que se les preguntará a las autoridades encargadas de las normas sociales ¿qué ocurrirá en el futuro? ¿Que pasara cuando los datos biométricos se hayan establecido de manera definitiva en nuestra manera de vivir?

Sin duda, debido a lo rápido que aparecen los avances tecnológicos e informáticos, estas preguntas no tienen respuesta. Es por esto que los ordenamiento jurídicos de las sociedades debe esta establecer garantías frente a

estos posibles vacíos o lagunas dentro del derecho, generando, mecanismos y herramientas que permiten una coexistencia entre de la tecnología biométrica y su disfrute de manera segura, pues aunque es difícil, ya que la realidad social siempre será más completa y amplia que el derecho, la normativa debiera ser capaz de anticiparse a la creación de las nuevas tecnologías, de las vulnerabilidades que surjan de esta, y por lo tanto ser capaz de crear mecanismos y herramientas que resguarden los derechos humanos.

Bibliografía

Comisión Interamericana de Derechos Humanos, OEA. (2017). *Estándares para una internet libre, abirta e incluyente.* Recuperado de http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf.

Convencion Americana sobre los Derechos Humano. (1969). *Pacto de San Jose.* San Jose de Costa Rica.

Diaz, M. (2018). *El cuerpo como dato.* Recuperado de https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf.

Domaica, J. (2019). *Datos Personales Bioemtricos Dactiloscopicos y Derechos Fundamentales: Nuevos retos para el Legislador* (tesis doctoral). Universidad Nacional de Educación a distancia, Madrid, España.

Garrido Iglesias, R., & Becker Castellaro, S. (2017). La biometría en Chile y sus riesgos. *Revista Chilena de Derecho y Tecnologia, volumen 6* (1) , 1-25.

Herrán Ortiz, A. I. (2003). *El derecho a la protección de datos sensibles en la sociedad de información* . Bilbao, España: Universidad de Deusto .

Korja, J. (2006). *The privacy risks of biometric identification.*, en *Society Trapped in the Network. Does it hav a future?* Recuperado de https://lauda.ulapland.fi/handle/10024/62488.

Muñoz Gallardo, S. (2017). *Datos Biometricos y Derechos Fundamentales* (tesis de grado) . Facultad de Derecho, Universidad de Chile, Santiago de Chile.

Naciones Unidas. (1948). *Declaración Universal de Derechos Humanos.* Paris.

ONU, Biometrics Institute. (2018). *Compendio de prácticas recomendadas de las Naciones Unidas* .

Asamblea General de Naciones (1966). *Pacto Internacional de Derechos Económicos, Sociales y Culturales.*

Quintanilla Mendoza , G. (2020). Legislación, riesgos y retos de los sistemas biométricos. *Revista chilena de Derecho y tecnologia, volumen 9* (1), 63-91.

Ruiz, M., Rodriguez, J., Olivares, J. (2009). Una mirada a la Biometrica. *Revista Avances en Sistemas e Informaticas 6* (2), 29 - 38.

Sanches, G., Rojas, I. (2012). Leyes de proteccion de datos personales en el mundo y la proteccion de datos biometricos. *Revista Seguridad, 13.* s/p. Recuperado de https://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93

Serratosa, F. (2008). *La Biometria para la identificacion de personas.* Recuperado de https://www.academia.edu/31531606/La_biometr%C3%ADa_para_la_identificaci%C3%B3n_de

_las_personas_Francesc_Serratosa_PID_00195448

Tapia Rodriguez, M. (2008). Fronteras de la vida privada en el Derecho Chileno. *Revista Chilena de Derecho Privado, 11,* 117-144.