EL IRISIDEN: MÁS ALLA DE LOS LÍMITES RAZONABLES DE LA SEGURIDAD

RESUMEN

La duda sobre si nos estamos acercando cada vez más al universo de Minority Report; un entorno dominado por los avances tecnológicos en el cual, la búsqueda de la seguridad más absoluta ha sacrificado algunos de nuestros derechos fundamentales parece ir encontrando una respuesta: Es el mundo que estamos creando.

Actualmente, la tecnología nos permite la utilización de diversas técnicas biométricas para identificar "sin papeles", sino a través de los rasgos fisiológicos o de conducta del individuo, las que se han convertido en un método internacional de identificación cuya "globalización" trae consigo un replanteamiento de cuestiones no solamente éticas sino también jurídicas, que nos enfrenta a dos grandes disyuntivas: "Seguridad de todos versus libertad de cada uno" y "Verificación de Datos personales o identificación indiscriminada de las personas".

Si bien en los últimos años se ha tornado en un proceso que complementaría la identificación electrónica, la Biometría, requiere de la intervención de muchos actores, estándares y normativas por lo que nos cuestionamos en torno a la posibilidad que tras la búsqueda de una seguridad física absoluta podamos generar una inseguridad jurídica total. Cuestiones ambas, que nos llevan a adentrarnos en la Biometría Informática y sus aplicaciones.

Palabras Clave: Biometría informática, Cibervigilancia, irisiden, datos personales

IRISIDEN: GO BEYOND THE REASONABLE LIMITS OF SECURITY

ABSTRACT

The doubt about being closer to Minority Report Universe, an environment controlled by technological advances in where the searching for the most complete security has sacrificed some of our fundamental rights seems to get a response: It is the world we are building.

Currently technology let us to use varied biometrics techniques to identify "without paper", otherwise through personal physiological characteristics or individual behavior, which have become an international method of identification bringing alone with its "globalization" reconsidering not only some issue ethics but legal ones. Both of them make us deal with two serious dilemma: "Security of all of us versus freedom of each one" and "Verify of personal data or people indiscriminate identification".

Even though during last years it has turn into a process which has made possible to complement electronic identification, biometrics required the intervention of many actors, standards and regulations, that is why we wonder about the possibility of trying to get a complete physical security we could get a total legal insecurity. These both issues take us to get tinto Informatic biometrics and its applications

Key words: Informatic Biometrics, Cibervigilance, irisiden, personal data.

I. INTRODUCCION

A lo largo de la historia, tanto personas como estados han centrado su preocupación en torno a la seguridad, sea por razones económicas, sociales, legales, entre otras. Uno de los factores que contribuyen a la consecución de esta seguridad gira en torno a la identificación y verificación de las personas. Con el paso de los años la tecnología ha proporcionado diversos métodos altamente seguros para lograr que estos procesos sean lo suficientemente fiables.

Debe tenerse presente que la identificación es un proceso a través del cual se asegura la identidad de otra persona o debe los lugares por los cuales nos desplacemos.

II. BIOMETRÍA INFORMÁTICA

La Biometría Informática ha sido definida como la aplicación de técnicas biométricas destinadas a la autentificación e identificación automática de personas en sistemas de seguridad informática. Las técnicas biométricas se basan en medir al usuario directa o indirectamente para reconocerlo automáticamente aplicando técnicas estadísticas y de Inteligencia Artificial.

La palabra biometría tiene dos significados:

- El concepto tradicional de biometría enmarcado dentro de una disciplina que se inició a principios del siglo XX y se refiere a la aplicación de las técnicas matemáticas y estadísticas al análisis de datos en las ciencias de los seres vivos, como la medicina o la biología.
- El contexto tecnológico de la palabra biometría se refiere a la aplicación automatizada de técnicas biométricas a la certificación, autentificación e identificación de personas en sistemas de seguridad. Las técnicas biométricas se utilizan para medir características corporales o de comportamiento de las personas con el objeto de establecer una identidad. Para diferenciar estos conceptos, organizaciones y autores han dado un nombre compuesto al contexto tecnológico como biometría informática y autentificación biométrica [1].

En consecuencia, está tecnología permite establecer una relación entre una persona y un determinado patrón asociado a ella de forma segura e intransferible. La diferencia principal de los métodos biométricos de identificación con los métodos clásicos radica en que la propia persona es la "llave". Dicha llave no puede ser perdida ni robada y su falsificación resulta cuanto menos costosa [2].

Podemos encontrar dos tipos básicos de biometría.

Biometría estática: mide la anatomía del usuario: Análisis del iris (irisiden), huellas digitales, geometría de la mano, termografía, venas de las manos, reconocimiento facial, patrones de la retina, etc.

Biometría dinámica: mide el comportamiento del usuario: Patrón de voz, firma manuscrita, cadencia del paso, análisis gestual, dinámica del tecleo, entre otros.

Debe considerarse que un indicador biométrico es alguna característica con la cual se puede realizar la biometría y que

no cualquier característica anatómica puede ser utilizada con éxito por un sistema biométrico ya que previamente debe cumplir con algunas características como serían:

- *Universalidad:* cualquier persona posee esa característica;
- *Unicidad:* la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña;
- *Permanencia:* la característica no cambia en el tiempo; y
- *Cuantificación:* la característica puede ser medida en forma cuantitativa.

Los requerimientos anteriores sirven como criterio para descartar o aprobar a alguna característica como *indicador biométrico*. Luego de seleccionar algún indicador que los satisfaga es necesario imponer restricciones prácticas sobre el sistema que tendrá como misión recibir y procesar a estos indicadores; las cuales apuntan, básicamente, a la obtención de un sistema biométrico con utilidad práctica. Las restricciones antes señaladas implican que el sistema considere:

° *El desempeño*, que se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales y/u operacionales. El objetivo de esta restricción es comprobar si el sistema posee una exactitud y rapidez aceptable con un requerimiento de recursos razonable.

° *La aceptabilidad*, que indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria. Es claro que el sistema no debe representar peligro alguno para los usuarios y debe inspirar "confianza" a los mismos. Factores psicológicos pueden afectar esta última característica. Por ejemplo, el reconocimiento de una retina, que requiere un contacto cercano de la persona con el dispositivo de reconocimiento, puede desconcertar a ciertos individuos debido al hecho de tener su ojo sin protección frente a un "aparato". Sin embargo, las características anteriores están subordinadas a la aplicación específica. En efecto, para algunas aplicaciones el efecto psicológico de utilizar un sistema basado en el reconocimiento de características oculares será positivo, debido a que este método es eficaz implicando mayor seguridad.

° *La fiabilidad*, que refleja cuán difícil es burlar al sistema. El sistema biométrico debe reconocer características de una persona viva, pues es posible crear dedos de látex, grabaciones digitales de voz prótesis de ojos, entre otros. Algunos sistemas incorporan métodos para determinar si la característica bajo estudio corresponde o no a la de una persona viva. Los métodos empleados son ingeniosos y usualmente más simples de lo que uno podría imaginar. Así por ejemplo, un sistema basado en el reconocimiento del iris revisa patrones característicos en las manchas de éste, un sistema infrarrojo para chequear las venas de la mano detecta flujos de sangre caliente y lectores de ultrasonido para huellas dactilares revisan estructuras subcutáneas de los dedos.

III. IRISIDEN: IDENTIFICACIÓN BASADA EN EL ANÁLISIS DEL IRIS

Aun pareciendo un sistema relativamente moderno, el uso del iris como medio de reconocimiento de personas nace a finales del siglo XIX para la identificación de criminales. Sin embargo, no es hasta finales de los años 80 cuando se retoma el estudio del reconocimiento de iris como medio eficaz de identificación.

Como señalamos anteriormente, Las técnicas biométricas usan características o comportamientos fisiológicos propios de cada individuo para identificarlo. El reconocimiento del iris es considerado como uno de los medios más certeros y fiables dentro de la biometría.

La importancia del iris radica principalmente en el carácter único e individual para cada persona, siendo esto una de las principales ventajas de su uso en el campo de la seguridad empresarial y valuarte de su éxito y propagación por numerosos países en el mundo. Esta técnica presenta una mayor unicidad que la huella y gran estabilidad por la protección de la córnea. Del mismo modo destaca también su carácter no invasivo, entendido como la capacidad para capturarlos rasgos biométricos (la imagen del iris) sin necesidad de usar un medio que entre físicamente en contacto con el sujeto analizado. Sin embargo, algunos lo consideran de alto coste e inicialmente incómodo para el usuario.

Teniendo en cuenta que las características en las que está basada, el patrón de la textura del iris ocular, permanece inalterable durante la vida del sujeto los resultados obtenidos son uno de los mejores en la actualidad [3]

En general, un sistema típico de reconocimiento del iris incluye: la captura de la imagen del iris, comprobar que el iris pertenece a una persona viva y el reconocimiento de dicho iris.

- *La captura de la imagen del iris* implica capturar una secuencia de imágenes del iris de un sujeto usando un sensor diseñado específicamente para dicha función.
- *Verificación* de la naturaleza viva de la imagen del iris, para evitar falsificaciones y comprobar que el iris pertenece a una persona viva y no es ningún video, o secuencia de imágenes, ojo de cristal o cualquier otro artefacto.
- *Reconocimiento del iris*, es la parte principal del sistema y se encarga de recoger las características más importantes de la imagen para su posterior comparación con los patrones almacenados en la base de datos.

El autor del algoritmo que actualmente usan la mayoría de sistemas es John Daugman. Actualmente la investigación en el campo del reconocimiento del iris está desarrollando numerosas técnicas con el propósito de mejorar la eficiencia y la rapidez.

IV. IMPLICANCIAS ACTUALES Y FUTURAS DE LA BIOMETRIA INFORMATICA

Hoy en día, el uso más extendido de la biometría informática está orientado a la seguridad y al control de las personas y de sus acciones; es decir, a ser un "Sistema Vigilante".

En este sentido, encontramos que esta tecnología se aplica tanto a sistemas de control de acceso a lugares de alta seguridad, zonas restringidas o control de fronteras, entre otros; como a conseguir mayor seguridad en los sistemas de comercio electrónico, pago electrónico a través de Internet, banca electrónica, DNI electrónico (e-DNI), validación de firmas digitales por medio de una llave biométrica, marketing personalizado, autenticación de personas en aplicaciones de voto electrónico y de voto por Internet entre otros e indiscutiblemente a la investigación criminal.

Sin embargo, su uso no sólo está limitado a éstas áreas, sino que también se está extendiendo a otro tipo de aplicaciones relacionadas con la interacción Hombre-

Máquina, de esta forma un ordenador puede controlar el cansancio o el estado de animo de determinadas personas para verificar si están capacitadas para llevar a cabo alguna acción midiendo los marcadores biológicos correspondientes (por ejemplo el control de la frecuencia de parpadeo de un conductor de automóvil), facilitar la labor de "fichar" a los trabajadores de la empresa evitando posibles fraudes con el sistema tradicional de fotocheck y en otros campos aún en desarrollo, estaría sirviendo a otros fines.

Considerando el notable aumento de la presencia de los identificadores biométricos en la vida cotidiana de los ciudadanos y su total aceptación en salvaguarda de la "seguridad de todos", podríamos atrevernos a sostener que en un plazo medio, en los países altamente tecnificados los alumnos tendrán que pasar un sistema de entrada biométrico en el colegio; los adultos encenderán los autos mediante un escáner que identificará su huella dactilar y los reconocerá como propietarios, y los padres deberán identificarse a la puerta de las guarderías para poder recoger a sus hijos. Por si fuera poco y para terminar de incursionar en una de aquellas utopías que desde siglos atrás concibieron a una "sociedad perfecta"; gracias a la domótica, un instrumento que acumulará toda la información técnica sobre la casa se activará mediante un escáner del iris, que podrá también utilizarse para permitir o impedir la entrada de visitantes; y si se dudaba de la efectividad del sistema debido a la falta de un banco de datos universal, con el uso de irisiden se evitará problemas tan sensibles como el intercambio de bebés al nacer en los hospitales, recordemos que desde nuestro nacimiento ya somos asimilados a una base de datos de rasgos biométricos, el irisiden haría posible el "rastreo" más fácilmente por el resto de nuestras vidas.

Las consideraciones anotadas distan mucho de ser una predicción futurista, basta dar una mirada a nuestro alrededor, para darnos cuenta que la biometría informática a través de sus diversas técnicas, poco a poco van ganando más espacio.

V. ENFRENTADO DOS GRANDES DISYUNTIVAS

Nos preguntamos hasta qué punto deviene en razonable sacrificar "la libertad de cada uno" en pro de "la seguridad de todos"- y paradójicamente y al mismo tiempo- "la inseguridad de cada uno".

El tema pasa por determinar si las políticas de seguridad están confrontadas por nuestro derecho a la libertad individual (seguridad vs. libertad), o si tal vez, tras un análisis de ponderación dentro de un nuevo contexto situacional, la seguridad se convierta en un derecho fundamental del cual derive el hasta ahora derecho inherente a la naturaleza del hombre: la libertad; ya que sería la única forma de preservar un derecho originario.

Está claro que nos enfrentamos al problema del tipo "donde fijar la línea" (where to draw the line), en el cual, los detractores de los derechos fundamentales argumentarán a su favor que las meras abstracciones no tienen un sustento real cuando se argumenta sobre cuestiones prácticas, olvidando que lo abstracto puede ser el modo científico o vulgar de enunciarlos. Sin embargo, los que propugnan la existencia de un nivel de seguridad total, en perjuicio de "algo llamado libertad" parecen ser los más.

Al ser la libertad un derecho fundamental que ha acompañado al hombre a lo largo de su vida, éste, parece no haber reparado en la existencia de posibles "restricciones" a dicho derecho, fuera de

aquellas derivadas de la comisión de algún delito; sin embargo, la biometría informática nos enfrenta a estas "restricciones" derivadas de la tecnología que -sin excluir al sector público-, actualmente, se encuentra en gran porcentaje en manos del sector privado y sus consecuente fines; y donde debe tenerse presente que mientras en la biometría activa el usuario es consciente de que le están tomando datos biométricos para ser registrado, en la biometría pasiva la persona no sabe que en ese momento preciso, hay un lector verificando que efectivamente es la persona que dice ser. En consecuencia; ¿se estarían vulnerando sus derechos?, ¿está constitucionalmente prohibido?.

En opinión de los mismos defensores de la biometría, el irisiden es una tecnología que nunca debe permitirse caiga en manos del gobierno ya que devendría en peligrosa para la privacidad y los derechos humanos.

Imaginemos una total intervención estatal en este contexto: seguridad y control de todos los ciudadanos por parte del estado con las consecuentes restricciones de los derechos por cualquier motivo que el estado considere necesario para el logro de sus fines, en otras palabras el irisiden realizaría una "función de rastreo de los ciudadanos", a merced de las "necesidades" del aparato estatal, lo que implicaría que una base de datos pueda encontrarnos en cualquier lugar del país, en cualquier momento, haciendo referencia específica a los lugares en los que estamos, las cosas que compramos, los libros que consultamos en una biblioteca o las personas con las que estuvimos durante el día, ¿la materialización del estado orweliano?.

Por otro lado, en cuanto a la identificación o verificación (autenticación) se refiere, el irisiden cuando es empleado en los procesos de identificación, es decir cuando responde a la pregunta: "¿quién es esta persona?", determina a un individuo comparando sus características biométricas con los datos registrados en una base de datos, por lo tanto, se compara "uno" a "muchos"; sin embargo, en los procesos de autentificación: "¿es seguro que es esta persona?", se trata de una comparación "uno" a "uno" entre las medidas biométricas grabadas en la tarjeta de quien se presenta y las medidas conocidas del supuesto individuo.

Evidentemente, nos encontramos con otro derecho fundamental que podría ser objeto de vulneración: la privacidad de las personas, que a su vez, puede implicar la manipulación o alteración de los datos personales para fines diversos; el irisiden justificaría atentar contra este derecho en virtud de la existencia de un elemental estado de sospecha sobre el individuo, pero ¿hasta dónde tenemos que extender el límite de la permisividad?. Si recordamos que las nuevas tecnologías han creado al llamado "ciudadano de cristal" parecerían incompatibles los términos: privacidad y seguridad, dado que el irisiden haría posible que los datos circulen con independencia de las personas a los que les pertenece.

Finalmente, si no existe límite para las nuevas tecnologías, ¿debería la legislación prever la aparición continuada de nuevos métodos o técnicas a efecto de evitar actos atentatorios contra nuestros derechos fundamentales?, creemos que no; sin embargo, será la correcta regulación jurídica de la utilización de las técnicas biométricas, y no su disponibilidad tecnológica o comercial, la que deberá dar la medida final de su valor como elemento adecuado en la protección y salvaguarda de nuestros derechos y libertades, ya que está claro, que la

biometría informática avanza viento en popa; pero, ¿está claro a donde nos está conduciendo?.

VI. CONCLUSIONES

En la medida que se implementan las diversas modalidades de biometría nos convertimos cada vez más en la "llave" de todos los sistemas, siendo fácilmente localizables y reconocibles donde sea que nos encontremos por lo que es innegable que en un futuro cercano los sistemas biométricos serán el único medio empleado para permitir el acceso e identificación de las personas y contradictoriamente para ejercer mecanismos de control sobre nosotros mismos. Llegado ese momento, el Derecho tendrá que enfrentar y dar respuesta a las posibles afectaciones o vulneraciones derivadas de la aplicación del irisiden. En este contexto tendrán un rol fundamental los estándares de certificación que se adopten para los dispositivos que se empleen.

REFERENCIAS BIBLIOGRAFICAS

[1] Gonzales, Eduardo, Introducción a los biométricos. Boletín Tress, julio 2005. Disponible en el sitio web http://www.tress.com.mx/boletin/julio2005/biometricos.htm-. Consultado el 5 de enero del 2016

[2] Picón Ruiz, Artzai. Robotiker, Técnicas biométricas para la identificación y verificación de las personas. Disponible en el sitio web http://revista.robotiker.com/revista/articulo.do;jsessionid=7F436FE61C1FB3C69821FD9208A3ACFC?method=detalle&id=67. Consultado el 5 de agosto del 2015

[3] Ruiz Marín, Milton; Rodriguez Uribe, Juan Carlos; Olivares Morales, Juan Carlos. Una mirada a la biometría. Revista Avances en Sistemas e Informática, vol. 6, núm. 2, septiembre, 2009, pp. 29-38. Universidad Nacional de Colombia. Medellín, Colombia. Disponible en el sitio web http://www.redalyc.org/articulo.oa?id=133113598005 Consultado el 12 de diciembre del 2015