

BIOMETRÍA E INVESTIGACIÓN CRIMINAL^{1,2}

BIOMETRICS AND CRIMINAL INVESTIGATION

Federico Bueno de Mata

Profesor Titular de Derecho Procesal.

Universidad de Salamanca. España.

E-mail: febuma@usal.es

RESUMEN. El trabajo se propone analizar la biometría en juicio, el concepto, la biometría como diligencia de investigación tecnológica, la biometría en España, la biometría del futuro y una propuesta hacia una ley de diligencias y datos biométricos.

PALAVRAS CLAVE. Biometría; Investigación Criminal; España.

ABSTRACT. The work aims to analyze biometrics in trial, the concept, biometrics as a technological research diligence, biometrics in Spain, the biometrics of the future and a proposal towards a law of proceedings and biometric data.

KEY WORDS. Biometrics; Criminal Investigation; Spain.

SUMARIO. 1. De la huella dactilar al dato biométrico como medio de identificación. 2. Concepto de biometría. 3. Biometría como diligencia de investigación tecnológica. 4. La biometría utilizada actualmente en España. 4.1 Retratos robot. 4.1.1 Limitaciones. 4.2. Reconocimientos fisionómicos y faciales. 4.2.1 Limitaciones del reconocimiento facial mediante racionalidad humana. 4.2.2 Limitaciones del reconocimiento facial mediante interfaz informática. 5. La biometría del futuro. 6. Hacia una ley de diligencias y datos biométricos. Referencias.

¹ Artigo recebido em 24/07/2020, sob dispensa de revisão.

² Trabajo documentado a través de la realización de una estancia de investigación en el centro de investigación de la Policía Nacional Española en el Centro de Canillas, Madrid, concretamente en la sección de biometría y bajo el asesoramiento del funcionario de policía D. Sergio Castro Martínez.

1. De la huella dactilar al dato biométrico como medio de identificación

El uso de la biometría en juicio cobra importancia mediática en España gracias al caso de Pablo Ibar, un español que lleva 24 de sus 46 años en prisión. Tras haber pasado 16 años en el corredor de la muerte, la Corte Suprema de Florida anuló su juicio y el 20 de enero de 2019 fue declarado de nuevo culpable por un triple asesinato cometido en Florida en 1994. La única prueba que sirvió al jurado popular para condenarle fue un video en el que parecía ver la cara de Pablo Ibar cometiendo el crimen, y en el que se apreciaron datos biométricos sobre los centímetros que separaban diferentes partes de su cara.

Si nos remontamos al año 2007 y nos dijeran el nombre de “Jaime Giménez Arbe” puede que de primeras ni nos inmutemos, pero si a la vez decimos que es autor de tres homicidios y de decenas de atracos y que se torna como uno de los delincuentes más mediáticos de los últimos años en España por actuar siempre disfrazado o bajo otra identidad, puede que a mucha gente le venga a la cabeza su pseudónimo, El Solitario.

Como él, centenas de delincuentes en todo el mundo siguen un *modus operandi* basado en el disfraz o en la deformación de rasgos físicos como forma de evadir la atribución de determinados delitos. Esto unido a la picaresca e inteligencia para dejar el menor rastro de evidencias inculpatórias hacen que la Policía y cuerpos de seguridad tengan que proceder a realizar unas diligencias de investigación más exhaustivas con el fin de atribuir la autoría de determinados delitos a estos criminales.

Como pauta general, las pruebas clave, y que funcionan de forma óptima en nuestro sistema judicial para atribuir la comisión de un delito a su presunto autor son dos; por un lado la prueba de ADN, una prueba científica con una fiabilidad casi absoluta y que se puede obtener cuando el autor deja en la escena del crimen algún resto biológico propio, (semen, saliva, sangre, cabello o sudor) y gracias a ello se consigue, en primer lugar, situar al delincuente en el lugar donde se produjo el delito, y en segundo lugar, si es posible conectar dicho resto biológico con la realización de esa conducta para atribuirle su autoría.

El principio fundamental sobre el que se basa esta tecnología es la existencia de características del ADN que son únicas en cada persona. El problema aquí es que en muchas ocasiones no se pueden conseguir dichas muestras por no existir en el lugar del

crimen, por lo que debemos intentar conseguir, gracias a las diligencias de investigación, una muestra de las huellas dactilares que estén plasmadas en la escena para atribuir la comisión del crimen por esta vía.

La huella dactilar posee también esa atribución unívoca al individuo. Existen numerosos estudios científicos que avalan la unicidad de la huella de una persona y, lo que es más importante, la estabilidad con el tiempo, la edad, etc. En estos aspectos es una técnica que le lleva mucha ventaja a las demás, debido a su siglo de existencia.

La huella digital de un individuo es definida por una compleja combinación de patrones de líneas, arcos, lazos, y círculos. Un lector de huellas lee la huella mediante el uso de una luz intermitente a través de una lámina de vidrio, sobre el cual el usuario ha plasmado uno o varios de sus dedos, cuya imagen se digitaliza.

Como vemos tanto la prueba de ADN como la huella dactilar son recursos muy fiables y muy difícilmente falsificables, sobre todo en cuanto a falsear nuestra composición molecular, opción a día de hoy imposible; mientras que en materia de huellas la cosa está más avanzada, es fácil ocultar tus propias huellas e incluso se han llegado a dar casos extremos en los que determinados delincuentes han procedido a injertarse los dedos de los pies en sus manos, pues no poseen las mismas características³.

El problema se presentaría cuando no dispongamos de ninguno de los dos elementos anteriores para identificar a un determinado sujeto; es decir cuando se agoten las vías de investigación por no disponer de huellas o muestras biológicas: en estos casos la Policía deberá hacer uso de las técnicas de biometría, término poco utilizado en nuestra jerga habitual y con tintes futuristas pero que empieza a ganar terreno como forma de investigación policial y que se basa en analizar determinadas características fisionómicas o de comportamiento .

Técnicas como los reconocimientos fisionómicos mediante imágenes cotejando características del rostro, como su forma, las orejas o el iris del ojo empiezan a ser ya una realidad en nuestro país, mientras que al mismo tiempo aún quedan por desarrollar otras técnicas biométricas potenciadas por las TICs. La tecnología, aunque ya bastante evolucionada, sigue aletargada para llegar a las diferentes sedes policiales

³ DEL POZO PÉREZ, M. “El ADN en la investigación policial: Casuística operativa”, conferencia impartida en el Curso de Verano Policía y Proceso Penal III, en Salamanca, Junio 2010.

La biometría informática, como a continuación analizaremos, abre nuevos horizontes a la hora de investigar las autorías de los diferentes delitos, se abren perspectivas para reconocer a potenciales delincuentes como mediante el escaneo de venas de las manos, reconocimiento mediante iris del ojo, dinámica de teclado, olor, su forma de andar o el análisis de su retina.

2. Concepto de biometría

La vía para realizar estas nuevas investigaciones se refunde en el vocablo biometría, pero, ¿a qué se refiere exactamente este novedoso y raro término? El término se deriva de las palabras griegas "*bios*" de vida y "*metron*" de medida y no sería otra cosa que la investigación basada en el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos, de esta forma esta técnica se basa en el reconocimiento de individuos mediante rasgos corporales únicos⁴.

En la biometría se distinguen dos grupos de registros biométricos: los fisiológicos o morfológicos y los conductuales. Los primeros, fisiológicos o morfológicos, serían aquellos que hacen referencia a rasgos o cualidades físicas inalterables y presentes en todas las personas que se traducen en patrones fijos, como son: huella dactilar, geometría de la mano, características del iris, patrones vasculares de la retina, mano, etc. Mientras que por otro lado los biométricos conductuales son aquellos que se soportan sobre características de la conducta del ser humano tales como: pulsaciones del teclado, discurso, dinámica de la firma, etc.

Si a lo anterior, ya novedoso y futurista de por sí, le sumamos el impulso de las Nuevas Tecnologías de la Información y de la Comunicación (TICs) tendríamos una autenticación biométrica aún más fiable para medir y analizar las características físicas y del comportamiento humano con ayuda de la informática.

La "*biometría informática*" sería la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para "verificar" identidades o para "identificar" individuos.

⁴ SÁNCHEZ CALLE, A. *Aplicaciones de la visión artificial y la biometría*, Editorial Dykinson, Madrid, 2005, págs. 10 y ss.

Hoy en día han aparecido diversas técnicas de verificación humana teniendo en cuenta diferentes rasgos biométricos. De la mayoría de ellas es posible disponer tanto de programas como de sensores que las soportan. Entre estas técnicas, las utilizadas con más frecuencia en la actualidad, y de las que se espera un uso masivo en el futuro, se encuentran, el reconocimiento de iris, el reconocimiento de huellas, el reconocimiento de voz y el reconocimiento de caras.

Otras, en cambio, son aún demasiado avanzadas para un uso en el espacio europeo, pero que en los próximos años pueden ser una realidad, tales como el escaneo de veas, que capturan imágenes del patrón del flujo sanguíneo o la termografía facial basada en cámaras infrarrojas que detectan patrones de calor creados por el flujo sanguíneo emitido por la piel, por poner algún ejemplo y en los que posteriormente nos detendremos⁵.

3. Biometría como diligencia de investigación tecnológica

La Firma Electrónica, en adelante FE, presenta una serie de ventajas en cuanto autenticación de documentos electrónicos no vistas hasta ahora, pero a mi parecer también padece una serie de defectos que a continuación mencionaremos. Para explicar nuestra crítica debemos partir de que toda firma electrónica está compuesta por dos claves, una privada y otra pública, que permiten identificar a la persona que ha firmado el documento. La clave privada es el *password* o contraseña que debemos introducir inicialmente para usar un dispositivo de firma electrónica, normalmente introducida por un programa de ordenador vinculado a un procesador de textos o mediante un programa vinculado a nuestro DNI electrónico. Esta clave privada activa y vincula los datos personales de una persona con su clave pública, la cual se compone de una serie de certificados reconocidos legalmente y que son emitidos por autoridades de certificación⁶.

La crítica propia que encontramos en una figura como la FE, es que por mucho que sea una clave privada propia y personal, nadie garantiza que esa clave de ese DNI electrónico pueda ser sustraída, manipulada o desenscriptada; lo que queremos decir con

⁵ MERINO TAPIADOR, M. Tecnologías biométricas aplicadas a la seguridad. Editorial Ra-Ma, pág 45 y ss,

⁶ CARRASCOSA LOPEZ, Valentín- “La nueva ley española de firma electrónica”- paginas 147 y siguientes.- *Edicao Especial 2009 de la Revista de Direito das Novas Tecnologías*.- Instituto Brasileiro de Política e Direito da Informática, Brasil, 2009.

esto es que puede que debido a un robo de clave o de DNI o, debido incluso, a alguna coacción o intimidación, puede que alguien firme algo por nosotros sin nuestro consentimiento e infringiendo la ley.

En la firma tradicional gracias al peritaje caligráfico o las nuevas técnicas biométricas podemos llegar a atribuir a ciencia cierta a quién pertenece dicha firma y bajo qué condiciones se firmó, incluso bajo qué condiciones anímicas o si fue una firma realizada mediante coacción o miedo; sin embargo en el frío mundo del ciberespacio la cosa se complica, debido a la inexistencia de peritos caligráficos electrónicos por ser una firma técnica. Por dicha razón opino que se debería reforzar la seguridad de esta figura optando por unas nuevas medidas aún más garantistas en cuanto a la comprobación de la identidad de los sujetos autores de este tipo de firma mediante estos mecanismos electrónicos.

Nuestro DNI electrónico incorpora en su *chip*, además de las claves y los datos de este tipo de firma⁷, nuestra huella dactilar escaneada, por lo que con un lector de huella podríamos otorgar una fiabilidad mayor; incluso, podríamos recurrir a técnicas mucho más avanzadas como la biometría⁸, técnica consistente en el uso de las tecnologías para medir y analizar las características físicas y del comportamiento humanas con propósito de autenticación. Concretamente el reconocimiento mediante el iris o la retina podrían dar unos buenos resultados. Por supuesto, debido a su alto coste, estas medidas no se podrían aplicar a día de hoy a todos los documentos electrónicos, por lo que estaría descartada su implantación a nivel de usuario; pero sí lo veríamos oportuno para aquellos acuerdos de mayor enjundia a nivel político europeo o para formalizar negocios o contratos que tienen como base una cuantía monetaria muy elevada.

4. La biometría utilizada actualmente en España

En la Comisaría General de Policía Científica, en el complejo de Canillas de la Policía Nacional, y concretamente, en la sección de Antropología Forense, podemos

⁷ ALONSO UREBA, A. y G. ALCOVER GARAU: "La firma electrónica", *Derecho de Internet. Contratación electrónica y firma digital*, (coordinadores) MATEU DE ROS, R. y J. M. CENDOYA MENDEZ DE VIGO Aranzadi, Pamplona, 2001, págs. 12 y ss.

⁸ STS (3ª) RC 5017/2003, 2 -7-2007. Pruebas biométricas

encontrar a los profesionales que se encargan de aplicar estas técnicas biométricas para el reconocimiento de presuntos delincuentes.

A priori, es una sección muy alejada de los tópicos equipos de investigación de las ficciones televisivas estadounidenses en cuanto a protocolos y parafernalias, pero totalmente a la altura en cuanto a formación y recursos humanos⁹. La principal diferencia entre los españoles y los agentes de la serie de televisión es que la brigada de la Policía Nacional está compuesta por científicos que ejercen de peritos, es decir, no participan en la investigación.

A día de hoy, las técnicas que se usan de forma frecuente para identificar a sujetos con falta de evidencias dactilares o biológicas son los retratos robots y los estudios fisionómicos de los individuos, cuando se dispone de ellos una imagen o un testimonio capaz de recordarlo y describirlo físicamente.

4.1 Retratos robot

Los retratos robot son pericias aproximativas y se hacen siempre en un último caso, cuando no hay ningún tipo de pista, puesto que normalmente se elaboran cuando se agotan las vías de investigación. La policía dispone de unos programas informáticos para elaborar este tipo de descripciones que contiene una lista de los rasgos faciales más relevantes, sus nombres son *Faces 3.0* y *Facette*, y, aunque completos, puede resultar bastante insuficientes.

La Policía española no suele utilizar el envejecimiento facial en los retratos robots como una técnica para identificar a criminales huidos desde hace años, y únicamente se ha utilizado dos veces para personas desaparecidas, aún así disponen de un programa que marca los rasgos sobresalientes de un rostro humano, las arrugas del envejecimiento natural y la influencia de otros factores, como la adicción a las drogas, la exposición habitual al sol o la aparición de enfermedades: pero su uso más corriente es para identificar a los asaltantes en los casos en los que haya, como requisito indispensable, al menos un testigo ocular.

⁹ DE URBANO CASTRILLO, E y MAGRO SERVET, V. en *La prueba Tecnológica en la Ley de Enjuiciamiento Civil*, Madrid, 2003, págs. 33 y ss.

4.1.1 Limitaciones

A día de hoy este tipo de pericias aproximativas está muy cuestionada, hasta por los miembros del propio Cuerpo Nacional de Policía, ya que reconocen que su fiabilidad es escasa y los recuerdos de los testigos oculares muchas veces no son lo suficientemente claros ni se plasman bien por parte de los agentes. Después de analizar y observar de primera mano los distintos programas de creación de retratos de este tipo, pienso que lo mejor para intentar obtener unos resultados óptimos sería que los propios testigos “fabricaran” ellos mismos los retratos en dependencias policiales, pues el uso de estos *softwares* no es complicado.

Aún así la Policía Nacional hace todo en cuanto puede para que estas pistas nos lleven a un buen resultado; a nuestro favor podemos decir que los agentes del Grupo de Estudios Fisionómicos de la Policía Nacional solo usan los programas asignados y no recurren a *Google* para realizar sus retratos: ya que aún es sonado en nuestro país el “error” que cometió el FBI al utilizar los rasgos de Gaspar Llamazares para crear la imagen actual del terrorista Bin Laden, o las fuertes críticas que ofreció el retrato robot de una desaparecida Madeleine McCann con unos años más.

Podemos decir que en los tiempos que corren los retratos robots no pasan por su mejor momento, ni para el reconocimiento de presuntos delincuentes ni para el hallazgo de personas desaparecidas debido a su escaso porcentaje de acierto, sin ir más lejos, solamente en dos ocasiones se ha realizado esta técnica con desaparecidos españoles y, en ambos casos el resultado fue idéntico: las personas siguen sin aparecer. Por todo lo anterior, y desde mi punto de vista, veo que los *softwares* utilizados son mejorables y por ello deberíamos plantearnos o avanzar en el perfeccionamiento de programas de creación de retratos o apostar preferentemente por otros sistemas de reconocimientos antropológicos o biométricos.

4.2. Reconocimientos fisionómicos y faciales

La identificación de características faciales o reconocimientos fisionómicos ha experimentado un fuerte impulso gracias a la evolución en la tecnología de vídeo multimedia y la captura de fotografía digital con una gran dosis de *megapíxeles*. Lo anterior se traduce en un aumento de cámaras fotográficas o cámaras de vídeo en los lugares de trabajo, calles, establecimiento y en el propio hogar. De esta forma, y como afirman algunas empresas dedicadas a este tipo de reconocimiento, se va disminuyendo de este modo el carácter intrusivo del sistema, ya que los sujetos están acostumbrados a la presencia de cámaras en lugares concretos y no sienten invadida su intimidad.

Todo esto unido a que nuestros rasgos faciales son propios y cuasi únicos de cada persona, imaginemos gemelos idénticos, nos hace fácilmente reconocibles por nuestra cara al ojo humano, para, de este modo proceder a un proceso de identificación de un determinado sujeto¹⁰. Actualmente la sección de Antropología de la Policía Nacional se encuentra alejada de la utilización de técnicas de reconocimiento digital mediante programas informáticos por el hecho de no disponer de suficientes recursos económicos destinados a la contratación de los mismos, y, a su vez, por no existir una tecnología lo suficientemente fiable para proceder a este reconocimiento por poseer una serie de dificultades o carencias que examinaré a continuación.

Por tanto, este tipo de identificación es considerada como la más natural dentro de los sistemas biométricos, puesto que se hace “a ojo”, es llevada a cabo por profesionales con un gran bagaje profesional y experiencia a sus espaldas y que raramente falla.

Este procedimiento de identificación realizado por los agentes se divide en dos tareas: detección y reconocimiento. La primera comprende la localización de las caras que existen en una fotografía o en una secuencia de vídeo, mientras que la segunda compara la imagen facial con imágenes de referencia almacenadas en una base de datos, en la que también se almacena la identidad de las personas asociadas a cada imagen de referencia, basándose en elementos estructurales presentes en las caras y que se definen como puntos clave como la boca la nariz o los ojos. Una vez obtenidos estos rasgos característicos, se comparan con los previamente almacenados y el resultado de la comparación verifica o descarta la identidad de la persona.

¹⁰ Información obtenida de la empresa pionera en España, F7 Corporation, puede consultar diversas cosas relacionadas con la biometría en su web www.f7corp.com

De esto se extrae una conclusión clara, que es necesaria una etapa previa de creación de bases de datos amplias. Por lo que, a mi parecer, es en lo que se debería avanzar con paso firme, para mejorar sobre todo los programas informáticos destinados a este reconocimiento facial para hacerlos más eficaces y fiables.

4.2.1 Limitaciones del reconocimiento facial mediante racionalidad humana

El reconocimiento facial tiene una serie de limitaciones unidas a los avances tecnológicos. Por un lado la calidad de los fotogramas realizados por una cámara es muy sensible y muchas veces puede plantear distorsiones de la realidad. Como estos reconocimientos se encuentran basados en analogías o discrepancias existentes entre dos imágenes, hay que saber apreciar si éstas si son debidas a que son dos individuos distintos o si son debidas a las condiciones de la toma de imagen: lente, distancia al foco, etc. Debido a todo lo expuesto con anterioridad, nunca podremos comparar métricamente una imagen con otra que no haya sido tomada exactamente en las mismas condiciones (misma distancia, misma lente, etc.).

A colación de lo anterior las distorsiones más comunes que se presentan en video y fotografía digital son las siguientes:

-Efecto barril.

Debida al tipo de lente empleado en la cámara. Este efecto es muy común en las grabaciones de seguridad y se basa en una distorsión de la imagen provocando la curvatura de objetos o personas en determinados elementos de la imagen, cuestión que se agudiza en las zonas periféricas de la imagen.

- Variaciones en el ángulo de captura.

La variación real solo se produciría en ángulos de captura verticales. , sería cuando tomas un fotograma o video de diferentes alturas, pues las variaciones de los distintos

segmentos del rostro varían según la altura, por lo que las distancias , por ejemplo entre la nariz, los ojos y el mentón pueden variar según la altitud a la que se encuentre la cámara o la imagen. En cambio cuando captas una imagen en un plano horizontal la imagen de la cara no varía, pero si presenta el problema de que es más fácil esquivarla o escaparse de su foco de grabación o captura.

4.2.2 Limitaciones del reconocimiento facial mediante interfaz informática

Si nos basamos en las limitaciones puestas por una de las empresas pioneras de reconocimiento facial mediante dispositivos electrónicos que tiene convenio con nuestra Policía Nacional, *F7FaceRecognitionSDK*, vemos como a día de hoy nos queda mucho que avanzar para aunar las TICs con estos sistemas de investigación y reconocimiento fisionómico.

Se producen limitaciones en cuanto a la posición de la cara, que debe ser preferiblemente de frente y con no más de una curvatura de 15 grados; a su vez no reconoce muchas expresiones por lo que se recomienda que la expresión de la cara sea neutra para ser reconocida, con lo que una simple sonrisa, o una persona extráfrica o con los ojos cerrados no podrían ser nunca identificadas por el programa informático.

Si a lo anterior sumamos que existen limitaciones en cuanto a el ángulo por el que entre la luz en la foto y a que no reconoce objetos extraños como gafas o barbas, podemos concluir que en nuestro país debemos avanzar aún mucho más para poder obtener unos programas de reconocimiento facial digital aceptables.

Lo demandado por los agentes de la propia sección de Antropología Forense sería unos programas con bases de datos inmensos y que hiciera un primer muestreo con una serie de caras con las que se pueda casar la imagen del sujeto, para en un control posterior que fueran los propios policías los que eligieran el más adecuado entre la muestra sugerida para así obtener una fiabilidad mayor.

5. La biometría del futuro

Aunque en España aún nos queda mucho por avanzar, en otros países, y sobre todo, en América, existen ya otros tipos de biometría más avanzada para la identificación de individuos. Aún así ya hay técnicas que se empiezan a probar en España, aunque aún en fase de desarrollo, como son:

En primer lugar, el reconocimiento mediante el iris del ojo. Sería hacer un escaneo digital del iris del ojo mediante fotografías, ya que el iris es una característica parecida a la huella dactilar, irrepetible de individuo a individuo., En España ya es factible esta técnica a través de nuestro pasaporte. Igualmente, el reconocimiento mediante pabellón auricular. Está basada en la distinción de la forma de la oreja y la estructura del cartílago, proyectando parte del oído externo en dos dimensiones, y tiene una forma de identificación parecida a la huella dactilar. Ya se empieza a utilizar en España en los centros de antropología, pero siempre con una técnica manual o a ojo y no digital. Igualmente, el reconocimiento mediante venas de la mano o de la retina. Captura imágenes del patrón del flujo sanguíneo tanto en la palma de la mano como en la retina, gracias a unos rayos infrarrojos, por lo que se considera una técnica invasiva. Está ya disponible, pero no es comercializado en nuestro país por su alto costo.

A la vez que los métodos anteriores, ya existen técnicas como la termografía facial según las partes del cuerpo que se enrojecen al mentir, el sensor de olor a través de detectar mentira por los químicos que emiten distintos poros de la piel o analizar patrones de movimiento de cada persona.

Esto sería simplemente algunas técnicas biométricas más futuristas a la hora de identificar presuntos delincuentes o personas desaparecidas, por lo que observamos tras leer estas nuevas modalidades de reconocimiento que aún nos queda mucho por andar en este terreno investigativo a nivel mundial¹¹.

6. Hacia una ley de diligencias y datos biométricos

Al igual que mejoran las TICs, el saber hacer y la picaresca de los delincuentes también avanza, por lo que muchas veces recurren al disfraz, la cirugía u otros mecanismos

¹¹ <http://www.itu.int/net/itunews/issues/2010/01/05-es.aspx>

para no ser reconocidos a la hora de cometer un delito. Este saber hacer de los malhechores va unido al intento de dejar el menor rastro de pruebas posibles en el lugar del crimen por lo que muchas veces pruebas que sirven para identificar fácilmente a alguien, como pueden ser las huellas dactilares o los restos biológicos que proporcionan muestras de ADN. De esta forma debemos acudir a nuevas y novedosas opciones para poder poner nombre y apellidos a las personas que trasgreden la ley. Esta solución se llama biometría.

Tras estudiar en qué consisten los sistemas biométricos y ver sus diferentes modalidades tanto presentes como futuras podemos concluir que no deja de ser un tema innovador y de un estudio más necesario y pormenorizado de aquí en adelante. Aún así se ve como las tecnologías introducidas hasta ahora no obtienen un nivel de acierto aceptable, por lo que se deberían invertir más recursos económicos destinados a la mejora y la potenciación de estos programas para ser ofrecidos a su vez a los centros policiales.

Se puede afirmar que la sección de Antropología de la Policía Nacional en España hace un trabajo excepcional, ya que no tienen apenas fallos en la identificación de individuos, lo que lo hace todavía aún mas meritorio viendo la escasez de nuevos medios que poseen.

La falta de recursos digitales e informáticos no empaña el buen hacer de un grupo que se sigue fiándose más de la capacidad humana para el reconocimiento de individuos que de la inteligencia artificial, por lo que en muchos casos a día de hoy se vería innecesaria su introducción en estas áreas policiales, aún así sería óptimo obtener una combinación entre las Nuevas Tecnologías y las capacidades profesionales de la policía para que los resultados fueran fiables totalmente; esto quiere decir, un primer muestreo hecho digitalmente, con el fin de obtener desde una base de datos una serie de individuos que casen con el que aparece en la foto o el vídeo, para luego proceder por los agentes mediante sus propias máximas de experiencia a reconocer al individuo en cuestión.

Por último creemos que estas técnicas pueden tener cabida legal en nuestro país a través de su inclusión como nueva diligencia de investigación tecnológica respecto al inicio de la ley 13/2015, de reforma de la Ley de Enjuiciamiento Criminal sobre diligencias de investigación tecnológica, e incluso de recabar datos biométricos y considerarlo como dato personal, lo que haría de aplicación el nuevo Reglamento Europeo

de Datos Personales, con lo que conjugando estas dos normativas se podría aventurar una nueva ley sobre biometría en el presente año 2020.

REFERENCIAS

- ALONSO UREBA, A. y G. ALCOVER GARAU: "La firma electrónica", Derecho de Internet. Contratación electrónica y firma digital, (coordinadores) MATEU DE ROS, R. y J. M. CENDOYA MENDEZ DE VIGO Aranzadi, Pamplona, 2001.
- CARRASCOSA LOPEZ, Valentín- "La nueva ley española de firma electrónica"-.- Edicao Especial 2009 de la Revista de Direito das Novas Tecnologías.- Instituto Brasileiro de Política e Direito da Informática, Brasil, 2009.
- DE URBANO CASTRILLO, E y MAGRO SERVET, V. en La prueba Tecnológica en la Ley de Enjuiciamiento Civil, Madrid, 2003.
- DEL POZO PÉREZ, M. "El ADN en la investigación policial: Casuística operativa", conferencia impartida en el Curso de Verano Policía y Proceso Penal III, en Salamanca, Junio 2010.
- MERINO TAPIADOR, M. Tecnologías biométricas aplicadas a la seguridad. Editorial Ra-Ma.
- SÁNCHEZ CALLE, A. Aplicaciones de la visión artificial y la biometría, Editorial Dykinson, Madrid, 2005.