Núm.
54/2009

LOS DATOS BIOMÉTRICOS Y SU UTILIZACIÓN COMO DATOS DE CARÁCTER PERSONAL: EL PRINCIPIO DE PROPORCIONALIDAD Y EL PRINCIPIO DEL CONSENTIMIENTO

Eugenio Gil López
Profesor adjunto de Derecho Informático de la Universidad Pontificia de Salamanca, campus de Madrid
Ex alumno del Curso Monográfico sobre Protección de Datos Personales del CEF

Extracto:

El presente artículo tiene por objeto analizar la aplicación a los denominados datos biométricos a la luz de la vigente Ley de Protección de Datos Personales, estudiando de forma concreta la inclusión del dato biométrico dentro del concepto de dato personal establecido por la ley, y la aplicación a estos datos de los esenciales principios contenidos en el Título II como son el principio de calidad de los datos y el principio del consentimiento.

Palabras clave: informática, dato personal, biometría, consentimiento, proporcionalidad.

Sumario

1. INTRODUCCIÓN

En el momento actual en el que se encuentra nuestra sociedad no puede negarse la gran importancia que ha adquirido la informática en el desarrollo de nuestra vida cotidiana. Su implantación en el ámbito de las actividades profesionales y empresariales no ofrece ninguna duda, de tal forma que casi no podríamos entender el desarrollo de nuestro trabajo diario sin estar pegados a un ordenador. Pero junto al ámbito profesional, la informática ha entrado de lleno en nuestra vida personal y familiar, realizando a través de ella (concretamente, a través de la contratación electrónica) numerosas actividades que nos permiten obtener un importante ahorro no solo en términos económicos sino también en materia de tiempo y comodidad.

Por lo tanto, parece claro que la informática nos ha reportado importantes y considerables ventajas, pero junto a ello queremos hacer hincapié en que también existen considerables peligros que poco a poco vamos descubriendo y que normalmente se tratan de atajar a través de medidas legislativas muchas veces tardías, porque, como siempre se dice, el legislador va y siempre irá por detrás de la tecnología. Uno de esos problemas a que hacemos referencia es el conocimiento exhaustivo sobre las personas y sus datos personales por parte de otras personas ya sean físicas o jurídicas y que pueden influir sin nuestro consentimiento en nuestro ámbito más privado e íntimo.

2. LA PROTECCIÓN DE DATOS EN ESPAÑA Y LOS DATOS BIOMÉTRICOS

En la última década ha cobrado una especial y significativa importancia la denominada protección de datos personales. Esta protección en palabras del profesor DAVARA [1] debe ser entendida como el amparo debido a los ciudadanos contra la posible utilización por terceros de forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que identificable con él afecte a su entorno familiar, social o profesional.

[1] DAVARA RODRÍGUEZ, Miguel Ángel. *La transposición de la directiva sobre la privacidad y las comunicaciones electrónicas*. Ed. Fundación Vodafone. Universidad Pontificia de Comillas, págs. 20-21.

En base a estas consideraciones, el origen de esta protección lo encontramos en el artículo 18 de nuestra Carta Magna [2], que en su apartado cuarto indica expresamente que los poderes públicos limitarán el uso de la informática para garantizar el derecho al honor y a la intimidad personal y familiar de las personas. La importancia de esta declaración se ve acrecentada a partir de la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, que consagra a la Protección de Datos como un Derecho Fundamental semejante a los recogidos en el Título I de la propia Constitución, indicando «...que atribuye al titular de los datos un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos...».

Pero el objeto de protección no debe ser considerado simplemente el derecho a la intimidad, sino lo que autores como DAVARA [3] han calificado el derecho a la privacidad, entendida esta como la pertenencia de datos a una persona, que no dicen nada de forma individual pero que unidos a otros pueden configurar un perfil del individuo que este tiene derecho a exigir que permanezca en su ámbito privado.

En nuestro ordenamiento, el mandato constitucional del artículo 18 se plasmó en la denominada Ley Orgánica para la Regulación y Tratamiento Automatizado de Datos de Carácter Personal (LORTAD) de 1992, que estableció un primer régimen jurídico aplicable en el ámbito de la protección de datos, pero en un momento en que no existía una auténtica conciencia social que otorgara verdadera importancia a los datos personales y a su vinculación con la protección del derecho a la intimidad. Esto hizo que durante un largo período de tiempo la aplicación y cumplimiento de la ley fuera muy limitado, haciéndose necesaria una revisión de la normativa aplicable. Esta revisión vino de la mano de la Directiva 95/46/CE relativa a la protección de las personas físicas respecto al tratamiento de datos de carácter personal y a la libre circulación de dichos datos, Directiva que ha dado lugar a su vez a nuestra ley vigente en materia de protección de datos que es la Ley 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal (LOPD).

2.1. ¿Qué entendemos por dato personal?

Nuestra LOPD define a estos como cualquier información concerniente a personas físicas identificadas o identificables [4].

Más explícito es el Real Decreto 1332/1994, de 20 de junio [5], al disponer que son toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

La Directiva de la Unión Europea ya citada, 95/46/CE, define los datos personales en términos semejantes a nuestra Ley de Protección de Datos, añadiendo que «...se considerará identificable

[2] Artículo 18 de la Constitución Española de 1978.

[3] DAVARA RODRÍGUEZ, Miguel Ángel. *Manual de Derecho Informático*. Ed. Aranzadi 2002, pág. 54.

[4] Artículo 3 a) de la Ley 15/1999, de 13 de diciembre, de Protección de Datos.

[5] Artículo 1.4 del Reglamento de desarrollo de la LORTAD, aún vigente en cuanto no esté en contradicción con la LOPD.

toda persona cuya identidad puede determinarse, directamente o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica...».

Sin embargo, tiene especial importancia el Considerando 26 de la Directiva, que en un intento de acotar el concepto añade que «...para determinar si una persona es identificable, hay que considerar el conjunto de medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona». Esta razonabilidad ha sido utilizada por algunas legislaciones estatales en las cuales se excluían aquellas formas de identificación que implican inversiones desproporcionadas de tiempo y dinero, cuestión esta que puede afectarnos en nuestro estudio de los datos biométricos, si bien los avances tecnológicos de los últimos años permiten llevar a cabo su análisis evitando las inversiones desmesuradas.

Partiendo del análisis de todas estas manifestaciones legales, lo que se extrae de forma clara es que el concepto de dato personal es un concepto amplísimo que abarca cualquier tipo de datos de una persona física y que no necesariamente han de ser datos íntimos, los cuales por supuesto están incluidos.

Este concepto amplio de dato de carácter personal nos lleva a analizar su posible extensión a los denominados datos biométricos, y en qué condiciones se le aplicaría a esos datos los principios básicos recogidos en el Título II de la Ley de Protección de Datos, cuestiones que pasamos a analizar en los puntos siguientes.

2.2. El dato biométrico y los sistemas biométricos.

Para comprender mejor qué son los datos biométricos, diremos que son los relativos a los aspectos físicos que mediante un análisis técnico, permiten distinguir las singularidades de los individuos, de tal manera que es imposible la coincidencia de tales aspectos en dos individuos una vez procesados (tales como las huellas digitales, el iris del ojo, la voz y demás) [6].

Se puede decir que la utilización de datos biométricos es la forma más antigua que se puede utilizar para identificar a una persona, ya que a esta se le identifica por su rostro. La importancia actual de la biometría viene dada fundamentalmente por el hecho de que la evolución técnica nos abre la posibilidad de almacenamiento de la información biométrica en bases de datos.

Durante mucho tiempo, y aún se mantiene esta idea en gran medida, la identificación biométrica estaba ligada al ámbito policial y a la persecución penal (especialmente en el caso de la huella digital), pero hoy en día su uso tiende a extenderse a muchos otro ámbitos y en muchas ocasiones conduce a importantes debates ético-morales (por ejemplo, la posible manipulación genética del individuo a través de su ADN).

[6] Newirt, K. *26 Conferencia Internacional sobre privacidad y protección de datos personales*. Polonia 14, 15, 16 de septiembre de 2004.

Por tanto, la biometría se basa en el análisis de datos relacionados con el individuo, y podemos clasificarla en tres grandes categorías [7]:

- Tratamiento basado en el análisis morfológico, tal y como las huellas digitales, la forma de la mano, la red venosa de la retina o el iris.
- El examen de las trazas biológicas, tales como el olor, la saliva, la sangre o el ADN.
- El tratamiento basado en el análisis de los comportamientos, como la dinámica de trazado de una firma o el golpeo sobre el teclado de un ordenador.

Prescindiremos en el presente estudio del tercer tipo de biometría al que hemos aludido, por considerar que quedaría fuera del ámbito de aplicación de la Ley de Protección de Datos que no analiza en ningún caso conductas o comportamientos. En relación con los otros dos tipos de biometría, diremos que la obtención de estos datos biométricos se realiza en una fase que se llama de inscripción, en la cual a través de un sensor se extrae el rasgo específico de usuario y se elabora una plantilla biométrica, de tal forma que lo que se almacena es esta plantilla en forma digital y no el dato biométrico en sí mismo considerado.

Una cuestión también importante desde el punto de vista de la protección de datos personales, es la forma de almacenamiento de las plantillas personales, que depende fundamentalmente de dos cuestiones, del tamaño de la plantilla y del tipo de aplicación que se vaya a dar al dato biométrico. Estas plantillas se pueden almacenar fundamentalmente de las siguientes formas:

- En la memoria de un dispositivo biométrico.
- En una base de datos central.
- En tarjetas de plástico, ópticas o inteligentes, que permiten a los usuarios llevar consigo sus plantillas como métodos de identificación [8].

Todos estos datos que venimos analizando deben ser considerados como datos de carácter personal, y así ha sido reconocido por la Agencia de Protección de Datos, por lo que les será de aplicación lo establecido en la LOPD. Ahora bien, aunque pudiera parecer lo contrario los datos biométricos son datos meramente identificadores que podrían asimilarse salvando las distancias al DNI o al NIF, y que en principio no revelan nuevas características referentes al comportamiento de las personas. Esta cuestión tiene especial trascendencia en cuanto al régimen aplicable especialmente materia del consentimiento exigible, si bien en relación con ello volveremos posteriormente al tratar de forma específica el principio del consentimiento recogido en el artículo 6 de la ley.

[7] WALTER, Jean Philippe. Algunos aspectos de protección de datos relativos a la utilización de datos biométricos en el sector privado. Noviembre 2004, *www.datospersonales.org*.

[8] Documento de trabajo sobre biometría del grupo del artículo 29 sobre protección de datos de 1 de agosto de 2003. Pág. 4. El grupo se constituyó en virtud del artículo 29 de la Directiva 95/26/CE, y es el órgano asesor comunitario independiente sobre protección de datos y vida privada.

La afirmación antes recogida de que los datos biométricos son datos meramente identificativos puede resultar extraña en relación con los denominados datos genéticos y, concretamente, con el ADN. En relación con este, la Agencia de Protección de Datos ha señalado que debe ser considerado como un dato relativo a la salud [9] y, por lo tanto, es un dato sensible incluido en el artículo 7.3 de la LOPD, que exige requisitos especiales en materia de consentimiento. Tal y como señala ETXEBERRÍA GURIDI [10], se distinguen dos tipos de ADN, el codificante que refleja diversas características de los sujetos, y el no codificante, el cual es prácticamente imposible que coincida de un sujeto a otro y que permite su identificación. Este último es el denominado vulgarmente como ADN basura, y de él difícilmente podrán extraerse datos sobre la salud o sobre las características especiales de la persona. Esto ha hecho que existan autores que consideren que únicamente debe ser aplicada la Ley de Protección de Datos en relación con el ADN no codificante, ya que el codificante no emitirá la identificación del sujeto y quedaría fuera del ámbito de aplicación de la ley. Esta restricción nos parece excesiva y en clara discrepancia con la Recomendación (97) 5 del Consejo de Ministros del Consejo de Europa, relativa a la protección de datos médicos, según la cual son tales todos los datos referentes a la salud de los afectados, e incluye en ellos a los datos genéticos de las personas sin ningún tipo de distinción.

Por lo tanto, si la ciencia establece las posibilidades de determinación de un sujeto, o de sus características, a través de dicha información, cualquiera que sea su clase, es indudable que la misma constituye dato de carácter personal.

3. LOS PRINCIPIOS DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y SU APLICACIÓN A LA BIOMETRÍA

Estos principios aparecen recogidos en el Título II de la ley bajo el epígrafe antes señalado: «Principios de la protección de datos».

No nos detendremos en el análisis de todos ellos por considerar que en la materia que nos ocupa existen tres de ellos que son los que pueden plantear mayores problemas o dudas en su aplicación, mientras que los restantes serían prácticamente de aplicación directa y no representan mayores problemas que los que se plantean en relación con la generalidad de los datos personales.

3.1. Dentro de lo que la ley califica como **principio de calidad** coexisten dos principios íntimamente relacionados entre sí como son el principio de proporcionalidad y el principio de finalidad. El primero de ellos lo encontramos en el apartado 1 del artículo 4 de la ley, en el que se establece que los datos de carácter personal solo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. El principio de finalidad por su parte, se desprende del apartado 2 al indicar que los datos de carácter personal no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

[9] Agencia de Protección de Datos. Memoria del año 2000, pág. 396.

[10] ETXEBERRÍA GURIDI, José Francisco. *La protección de datos de carácter personal en el ámbito de la investigación penal*. Agencia de Protección de Datos. Madrid 1998, pág. 177.

En este mismo sentido se manifiesta el artículo 6 de la Directiva 95/46/CE, al señalar que los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. Además, los datos personales serán adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente.

Estos principios prohíben de forma tajante que los datos biométricos (y por extensión cualquier otro dato personal) puedan ser obtenidos de forma aleatoria e indiscriminada, siendo necesario fijar de forma clara, en primer lugar, los fines para los que se van a recoger y tratar los datos biométricos, y, en segundo lugar, solo podremos recoger y tratar los datos adecuados de acuerdo con los fines previamente determinados. Esta cuestión nos llevará inevitablemente a evaluar los riesgos que puedan producirse para los derechos y libertades fundamentales de las personas, y la posibilidad de obtener los fines perseguidos a través de una manera menos intrusiva para los sujetos que la utilización de la biometría [11]. Por tanto, no es posible obtener o conservar los datos biométricos para fines distintos a los determinados previamente y mucho menos para establecer perfiles genéticos de la población o mantener bancos de ADN sin el consentimiento de los afectados para la investigación de futuras conductas criminales.

Los datos biométricos son ampliamente utilizados en la actualidad con fines identificativos (en el pasaporte y DNI españoles como el rostro y la huella digital, así como el ADN en el ámbito de la investigación criminal), y con fines de control de acceso. En relación con estos y en aplicación del artículo 4 de la ley, el uso de estos datos no podrá ser utilizado en ningún caso para evaluar el estado emocional del interesado o para vigilarlo en el lugar de trabajo, ya que no sería compatible con los fines originales de la recogida.

Asimismo, el Grupo del artículo 29 de la Directiva 95/46/CE sobre protección de datos, ha señalado que lo deseable sería no almacenar la biometría en una base de datos, sino más bien solo en un objeto disponible exclusivamente para el usuario, como una tarjeta con microchip, un teléfono móvil o una tarjeta bancaria.

En los últimos años especialmente a partir de los terribles acontecimientos acaecidos en Nueva York, Madrid y Londres, se ha planteado la posibilidad de la utilización de los datos biométricos con una finalidad de prevención antiterrorista a través del intercambio de tales datos entre los diferentes países. Consultado sobre esta cuestión, el ex director de la Agencia Española de Protección de Datos, José Luis Piñar, ha señalado en relación con esta materia que sería necesario la aprobación de una norma clara, precisa, que dejase muy claro quién va a poder tratar esos datos, en qué casos, qué tipo de datos, qué se va a hacer con ellos, quién va a poder acceder a ellos, durante cuánto tiempo van a estar disponibles, y cuándo van a tener que ser cancelados o destruidos.

Este principio de calidad en las dos vertientes antes mencionadas, ha sido aplicado por la Agencia de Protección de Datos española en numerosos informes y resoluciones, sirva de ejemplo el Informe 368/2006 sobre la proporcionalidad del tratamiento de la huella dactilar de alumnos de un colegio. En el caso en cuestión, la Agencia Española de Protección de Datos consideró que la utilización

[11] Documento de trabajo sobre biometría del grupo del artículo 29 sobre protección de datos de 1 de agosto de 2003, pág. 6.

de la huella dactilar para establecer un sistema de control de los retrasos y ausencias de los alumnos, es desproporcionado con la finalidad perseguida, concluyendo que tal finalidad puede conseguirse de una manera menos intrusiva para los alumnos.

Sin embargo, una postura contraria a la anteriormente expuesta (aunque en casos que no guardan una identidad total de razón), puede verse en otras Resoluciones de la Agencia, donde de forma reiterada sí ha considerado ajustado al principio de calidad la utilización de la huella dactilar de los trabajadores para la comprobación de la identidad de los mismos, y el cumplimiento de su jornada laboral. En este sentido, sirvan de ejemplo las Resoluciones R/00619/2006 y R/00174/2006, donde sí se considera proporcionado la utilización de la huella dactilar como mecanismo de control. Por supuesto que en estos supuestos será requisito imprescindible para la legalidad de la actuación cumplir con los restantes principios de la ley, especialmente el ya mencionado de información (art. 5) y el del consentimiento (art.6) que analizaremos posteriormente.

Lógicamente, la diferencia entre los dos supuestos anteriores es notable y la encontramos en la especial consideración que debe tener el legislador y los poderes públicos con los menores de edad (con independencia de la existencia en el caso de los trabajadores de un contrato laboral) para preservar su intimidad, consideración especial que a su vez de modo acertado refleja nuestro legislador en el ámbito de protección de datos en la regulación que incorpora en el artículo 13 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley de Protección de Datos, en relación con el consentimiento para el tratamiento de datos de menores de edad.

Es decir, tanto en los casos planteados como en todos los relativos a los datos biométricos y en aplicación del principio de calidad, serán utilizados únicamente los datos imprescindibles para la finalidad establecida, y sería necesario acreditar que su utilización es necesaria para alcanzar tal finalidad.

3.2. Un segundo **principio** recogido en la ley es el **principio del consentimiento** (art. 6 de la ley). No es preciso recordar en este punto la importancia de este elemento en el ámbito de la protección de datos, constituyéndose en uno de los elementos sobre los que se articula la ley. La regla básica en principio es clara; salvo las excepciones tasadas que recoge la ley, nadie puede tratar nuestros datos personales sin contar con nuestro consentimiento (entendido el tratamiento en el concepto amplio que se recoge en el art. 3 de la ley).

Dada la importancia que se otorga al consentimiento, el legislador se ha preocupado de establecer una definición del mismo en el artículo 3 de la ley ya citado, donde se califica al consentimiento como una manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le conciernan [12]. Sin ánimo de extendernos en este concepto y por la importancia que tiene en relación con la biometría, simplemente indicaremos una serie de ideas en relación con dos de los caracteres contenidos en la definición legal. En ella se recoge la idea de que el consentimiento debe ser específico, es decir, debe recogerse para un determinado tratamiento que debe ser informado al usuario, lo cual nos pone en íntima conexión con el principio de finalidad del artículo 4 de la ley que hemos analizado anteriormente. Entendemos de acuerdo con los dos caracteres citados que el consentimiento debe ser recabado para finalidades determinadas, explícitas y legítimas.

[12] Artículo 3 h) de la Ley 15/1999, de 13 de diciembre.

Las dos primeras cuestiones hacen referencia al hecho de que la finalidad debe ser concreta (en su defecto la manifestación de voluntad no podrá ser específica), y la legitimidad se refiere al hecho de que el responsable del tratamiento debe estar legitimado para realizar el tratamiento para el cual solicita el consentimiento [13].

La segunda cuestión que queremos tratar de la definición de consentimiento es la consideración de que la voluntad debe ser inequívoca. El artículo 6 de la LOPD en su apartado 1 establece que para el tratamiento de los datos personales se requerirá el consentimiento inequívoco del afectado salvo que la ley disponga otra cosa, recogiendo el apartado 2 de este artículo una serie de excepciones a este principio.

El término inequívoco hace referencia a aquello que no admite duda o equivocación[14], y en el ámbito de la protección de datos se ha venido admitiendo por la Agencia de Protección de Datos y por los tribunales dos tipos de consentimiento que serían también válidos en el ámbito de los datos biométricos:

- Consentimiento expreso. Es el que resulta de un acto de declaración de la voluntad.
- Consentimiento tácito. Es el que se produce cuando pudiendo realizar una manifestación contraria, esta no se realiza.

En ambos casos el consentimiento prestado puede ser inequívoco, pues es necesario diferenciar entre las formas de recogida del consentimiento (expreso o tácito) con el carácter inequívoco del mismo [15].

Tal y como hemos señalado anteriormente, los datos biométricos en la mayoría de las ocasiones son meramente identificadores del individuo y no suelen ofrecer datos adicionales sobre el perfil de los mismos. Por tanto, en el ámbito de la biometría la regla general nos indica que cualquier tipo de consentimiento prestado de forma inequívoca por el afectado sería suficiente para el tratamiento de los datos. Pero como en derecho toda regla general contiene excepciones, debemos acudir al artículo 7 de la ley donde se regulan los denominados no muy acertadamente datos especialmente protegidos. Una primera lectura del precepto podría hacernos pensar que la biometría quedaría fuera de su ámbito de aplicación, sin embargo, es necesario realizar una serie de precisiones.

El artículo 7 establece que los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual solo podrán ser recabados, tratados y cedidos cuando, por razones de interés general así lo disponga una ley o el afectado consienta expresamente [16]. En términos semejantes se manifestaba el artículo 8 de la Directiva 95/46/CE. Por tanto, para estos datos ya no se admite el consentimiento tácito al que antes hacíamos referencia; o el consentimiento se obtiene a través de una declaración de voluntad expresa del afectado, o se habrá incurrido en una infracción de las conteni-

[13] Alonso Martínez, Carlos. *Protección de datos de carácter personal. El consentimiento en entidades financieras*. Ed. ASNEF. 2002, pág. 68.

[14] Diccionario de la Real Academia de la Lengua Española.

[15] Alonso Martínez, Carlos. *Protección de datos de carácter personal. El consentimiento en entidades financieras.* Ed. ASNEF. 2002, pág. 72.

[16] Artículo 7, apartado 3, de la Ley 15/1999, de 13 de diciembre.

das en el título VII de la ley con las consecuencias que ello lleva aparejadas. Así, debemos recordar en este punto la afirmación antes mantenida de que los datos genéticos eran datos de salud (por ejemplo, el ADN), y por tanto a todos ellos les sería de aplicación el régimen jurídico contenido en el artículo 6 de la ley en conexión con el 7.3, exigiéndose consentimiento expreso para su tratamiento. Asimismo, podemos entender que en sistemas biométricos basados en el reconocimiento facial, se pueden tratar los datos que revelan el origen racial o étnico [17], en cuyo caso consideramos que deben aplicarse igualmente las garantías establecidas en el artículo 7 de la ley.

Ahora bien, esto no significa que todo tratamiento de datos biométricos vaya a incluir datos sensibles, es más, lo normal debe ser lo contrario. Al final, si un tratamiento contiene datos biométricos o no, es una cuestión de apreciación vinculada con la característica biométrica utilizada y la aplicación biométrica en sí.

Una de las cuestiones que debe tratarse en el ámbito del consentimiento de los datos biométricos, son las posibilidades que existen para efectuar el tratamiento de dichos datos sin consentimiento del afectado. Piénsese, por ejemplo, en el supuesto de los datos (huella digital, ADN...) obtenidos en el ámbito de una investigación criminal e incluso la utilización de datos genéticos con fines meramente identificativos. En relación con estas cuestiones debemos citar el Convenio de PRUM de 27 de mayo de 2005, ya ratificado por España, relativo a la profundización de la cooperación transfronteriza, en particular en materia de la lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal. La finalidad de este es crear un marco de intercambio de datos personales para luchar conjuntamente contra los problemas citados [18]. El convenio establece que se podrán intercambiar datos personales «cuando la existencia de condenas firmes o de otras circunstancias justifiquen la presunción de que estas personas van a cometer un delito con motivo del evento o suponen una amenaza para la seguridad y el orden público, en la medida de que la transmisión de tales datos sea admisible con arreglo al derecho interno de la parte contratante transmitente [19]», lo cual nos lleva nuevamente a la aplicación en toda su extensión de nuestra Ley de Protección de Datos.

El convenio regula de forma expresa el ADN calificándolo como un dato de salud, pero sin embargo se refiere el convenio únicamente a la parte no codificante, que como hemos señalado es un identificado único fiable, mientras que el ADN codificado, que contiene la información relativa a enfermedades, queda fuera de las bases de datos del convenio.

En cuanto a los datos antes señalados utilizados en el ámbito de una investigación criminal, entendemos que será de aplicación el artículo 22 de la Ley 15/1999, de 13 de diciembre, de Protección de Datos, sobre ficheros de las Fuerzas y Cuerpos de Seguridad, en cuyo apartado 2 establece que: «La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad».

[17] Documento de trabajo sobre biometría del Grupo del artículo 29 sobre protección de datos de 1 de agosto de 2003, pág. 11.

[18] Artículo 1.1 del Convenio de PRUM de 27 de mayo de 2005.

[19] Artículo 12.1 del Convenio de PRUM de 27 de mayo de 2005.

En este precepto nos encontramos con una declaración en parte bastante parecida a la que vimos antes en el propio Convenio de PRUM.

Pero el apartado 3 del mismo artículo 22 hace referencia expresa a los datos sensibles del artículo 7, dentro de los cuales se incluyen los datos de salud como el ADN. Este apartado indica que: «la recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales».

Es decir, en relación con los datos de salud la ley exige por una parte que sean absolutamente necesarios, lo cual nos lleva a pensar que no hay otra forma menos intrusiva de resolver un determinado caso criminal, y deben estar relacionados con una investigación concreta que habrá que justificar, sin que sea posible alegar la declaración genérica del apartado segundo donde se hacía referencia a un peligro real para la seguridad pública o para la represión de infracciones penales.

Asimismo, es importante analizar si es posible el tratamiento de los datos biométricos sin el consentimiento de los interesados a través de alguna de las excepciones contenidas en el apartado 2 del artículo 6 de la ley referido al consentimiento. Esta cuestión en todo caso debe ser analizada conjuntamente con el principio de proporcionalidad ya visto, determinando si el tratamiento del dato biométrico en cuestión es excesivo para el fin que lo motiva. El problema se ha planteado en la práctica fundamentalmente en el ámbito de la huella digital, discutiéndose la posibilidad del tratamiento de la huella de funcionarios para la comprobación de su identidad y por extensión el cumplimiento de su jornada de trabajo. En este sentido, teniendo en cuenta que el tratamiento trae su origen, precisamente en la necesidad de asegurar el cumplimiento de las obligaciones derivadas de la relación estatutaria del funcionario con la Administración, la Agencia de Protección de Datos ha considerado posible su tratamiento inconsentido en base a las excepciones del artículo 6 apartado 2 de la misma en el que se prevé que no será necesario el consentimiento cuando los datos se refieran a las partes de un contrato o precontrato de una relación laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento [20].

Como conclusión, simplemente restaría afirmar de forma clara, tal y como lo ha hecho la Agencia de Protección de Datos Española, la aplicación de la Ley de Datos Personales en toda su extensión a lo que se ha venido a llamar datos biométricos, teniendo siempre presente que se debe tener una vigilancia constante de que la utilización de la biometría no pueda llegar a ser desproporcionada por su intima conexión con la privacidad del individuo, con la finalidad propuesta.

Asimismo, se debe tener en cuenta que la constante evolución de la técnica dará lugar a la aparición de nuevos datos biométricos, más complejos y en ocasiones más intrusivos, lo que nos obligará a realizar un análisis pormenorizado de la regulación legal de cada uno de ellos y la aplicación de la normativa de protección de datos.

[20] Agencia de Protección de Datos. Informe 1999-0000, *https://www.agpd.es/index.php?idseccion=136*.