AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Informe 0392/2011

I

La consulta plantea la conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre, del tratamiento de los datos necesarios para el reconocimiento de los alumnos de un determinado centro universitario a través de programas de reconocimiento facial, que se utilizarán para el control de su asistencia a las clases y la identificación de los mismos en la realización de las correspondientes pruebas.

El estudio de la cuestión planteada exige analizar, con carácter general, los supuestos de tratamiento de los datos biométricos y su viabilidad desde el punto de vista de la aplicación de las normas reguladoras del derecho fundamental a la protección de datos de carácter personal, con carácter previo a establecer una solución al caso concreto que aquí se plantea.

En primer término, y como viene señalando esta Agencia Española de Protección de Datos, cabe entender por datos biométricos “aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos en un sujeto y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión. Así se emplean para tales fines las huellas digitales, el iris del ojo, la voz, etc”.

Al propio tiempo, como recuerda el documento de trabajo sobre biometría, elaborado por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE, adoptado el 1 de agosto de 2003 (documento WP80), el tratamiento de dichos datos ha evolucionado desde la referencia esencial a aquéllos datos que pueden ser considerados como “estáticos”, es decir, invariables a lo largo de la vida de la persona, como su huella genética, su huella dactilar o el iris, a otros que podrían denotar determinadas características de su comportamiento, tales como la forma de andar o el olor desprendido por el sujeto.

Centrándonos en los datos de carácter “estático” y ateniéndonos a la definición de dato de carácter personal contenida en el artículo 3 a) de la Ley Orgánica 15/1999, debe indicarse que si bien el procesamiento de estos datos biométricos no revela nuevas características referentes al comportamiento de las personas sí permite, lógicamente, su identificación, dado que, como se analiza en el documento del Grupo del artículo 29, en un gran número de supuestos su finalidad es precisamente la identificación del sujeto o el control

de acceso a una determinada instalación o puesto de trabajo. Por ello, resulta evidente que, en caso de procederse a su tratamiento dicho tratamiento deberá ajustarse a la Ley Orgánica 15/1999.

Al propio tiempo, el análisis acerca del posible tratamiento de estos datos no debe partir de un principio inicial de oposición al mismo, resultando, como también se señala en el tan mencionado documento, dicho tratamiento sumamente útil para preservar en un gran número de ocasiones la intimidad del propio afectado, al hacer innecesario el tratamiento de otros datos adicionales.

En este sentido, la evolución de la tecnología ha demostrado la utilidad del tratamiento de datos biométricos en el desarrollo de sistemas de identificación única de la población. En este sentido, no debe olvidarse el tratamiento de datos biométricos que en la actualidad tiene lugar para la emisión del Documento Nacional de Identidad electrónico o del Pasaporte, ras la reforma operada por el Real Decreto 896/2003, de 11 de julio, cuyo artículo 10.5 dispone que “Igualmente se podrán incluir datos biométricos que sean necesarios para una más completa identificación del titular, insertándose bien en la página de datos personales, referida en el apartado 2 de este artículo, o bien en la que se determine por el Ministerio del Interior”.

Igualmente, debe tenerse en cuenta el Reglamento (CE) núm. 2252/2004, de 13 de diciembre, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros.

II

Dicho esto, y entrando en el análisis del tratamiento al que se circunscribe la consulta que motiva la emisión del presente informe, será preciso, siguiendo nuevamente el documento WP80 tomar en consideración como elementos esenciales para juzgar la conformidad de dicho tratamiento con las previsiones de la Ley Orgánica 15/1999 los principios de legitimación para el tratamiento de los datos y finalidad, en las distintas previsiones que en relación con éste último establece el artículo 4 de la Ley Orgánica.

Así, será necesario que el tratamiento se encuentre habilitado por alguna de las causas que en el derecho español autorizan el mismo. En particular, el artículo 6.1 de la Ley Orgánica dispone que “el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”. Fuera de estos casos, dispone el artículo 6.2 que “no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la

satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".

De estas causas legitimadoras del tratamiento debe descartarse la referente al consentimiento del interesado, habida cuenta del carácter esencialmente revocable del mismo, tal y como prevé el artículo 6.3. En efecto, teniendo en cuenta la finalidad de control perseguida, no puede considerarse admisible un sistema basado en el consentimiento del afectado, dado que en caso de que aquel voluntariamente quisiese revocar el tratamiento, lo que implicaría la necesaria cesación en el tratamiento de los datos por parte del responsable, no sería posible el cumplimiento de la finalidad perseguida.

Igualmente, como es lógico, el tratamiento de datos biométricos no podrá fundarse en su inclusión en fuentes accesibles al público y, previsiblemente, salvo en supuestos concretos como los relacionados con la huella genética del afectado, no será necesario para atender un interés vital de aquél.

Ello implicará que el tratamiento deberá encontrarse habilitado en una norma con rango de Ley, en el sentido amplio que se ha venido manteniendo por esta Agencia Española de Protección de Datos y establece el artículo 10.2 a) del Reglamento de desarrollo de la Ley Orgánica 15/1999, o que el mismo sea necesario para el adecuado mantenimiento de una relación jurídica, en los términos previstos en el artículo 6.2 de la Ley Orgánica.

En la mayor parte de los supuestos, como el que se plantea en la consulta, podrá aducirse la necesidad del tratamiento para el mantenimiento de una relación jurídica entre quien trata el dato y el afectado. Así ha sucedido en los distintos casos sometidos hasta la fecha al parecer de la Agencia, a los que posteriormente se hará referencia, si bien relacionados sobre todo con el tratamiento de la huella dactilar. De este modo, se viene a considerar por el responsable que la preexistencia de un vínculo jurídico, contractual o de otra índole, con el afectado posibilita el tratamiento de la huella dactilar, a fin de poder procederse al efectivo control del cumplimiento por el afectado de las obligaciones derivadas de esa relación jurídica.

Además, debe tenerse en cuenta el efecto derivado de la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, que ha declarado expresamente el efecto directo del artículo 7 f) de la Directiva 95/46/CE, según el cual "Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (...) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva". Por ello, dicho precepto deberá ser tomado directamente en cuenta

en la aplicación de la normativa de protección de datos de carácter personal por los Estados Miembros, y en consecuencia por esta Agencia Española de Protección de Datos, dado que como señala el Tribunal Supremo en su sentencia de 8 de febrero de 2012 “produce efectos jurídicos inmediatos sin necesidad de normas nacionales para su aplicación, y que por ello puede hacerse valer ante las autoridades administrativas y judiciales cuando se observe su trasgresión”.

Tal y como recuerda la Sentencia del Tribunal de Justicia de la Unión Europea en su apartado 38, el artículo 7 f) de la Directiva “establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado” y, en relación con la citada ponderación, el apartado 40 recuerda que la misma “dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado”.

Por este motivo, la sentencia señala en su apartado 46 que los Estados miembros, a la hora de adaptar su ordenamiento jurídico a la Directiva 95/46, deberán “procurar basarse en una interpretación de ésta que les permita garantizar un justo equilibrio entre los distintos derechos y libertades fundamentales protegidos por el ordenamiento jurídico de la Unión, por lo, conforme a su apartado 47 que “nada se opone a que, en ejercicio del margen de apreciación que les confiere el artículo 5 de la Directiva 95/46, los Estados miembros establezcan los principios que deben regir dicha ponderación”.

Por tanto, para determinar si procedería la aplicación del citado precepto habrá de aplicarse la regla de ponderación prevista en el mismo; es decir, será necesario valorar si en el supuesto concreto objeto de análisis existirá un interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos que prevalezca sobre el interés o los derechos y libertades fundamentales del interesado que requieran protección conforme a lo dispuesto en el artículo 1 de la Ley Orgánica 15/1999, según el cual “la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar” o si, por el contrario, dichos derechos fundamentales o intereses de los interesados a los que se refiera el tratamiento de los datos han de prevalecer sobre el interés legítimo en que el responsable pretende fundamentar el tratamiento de los datos de carácter personal.

III

Ello conduce al necesario análisis de los distintos principios vinculados con la finalidad que justifica el tratamiento, a los que se hizo referencia con anterioridad y que, en particular, debe materializarse en los principios de proporcionalidad y prohibición del tratamiento con fines incompatibles a los que justificaron la recogida y tratamiento de los datos, consagrados en los artículos 4.1 y 4.2 de la Ley Orgánica 15/1999. Ello se funda en que de producirse una situación en que la aplicación de los citados principios aparezca forzada será posible entender que el tratamiento de los datos causa un perjuicio a los derechos de los interesados de tal magnitud que no podrá justificarse el tratamiento de los datos en la mera invocación del interés legítimo del responsable o en la mera relación jurídica que vincula al afectado con aquél, al ser mayor el perjuicio causado que el interés perseguido con el tratamiento.

Como establece el artículo 4.1, “los datos de carácter personal sólo 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”. A su vez, conforme al artículo 4.2, “los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos”.

La aplicación del principio de proporcionalidad aparece directamente vinculada, como se ha indicado, a la invocación como causa del tratamiento del principio de necesidad para el mantenimiento o cumplimiento de una determinada relación jurídica o a la invocación del interés legítimo, resultando menos relevante en caso de que el legislador haya habilitado expresamente este tratamiento, toda vez que en ese caso corresponderá al propio legislador y, en su caso, al tribunal Constitucional, la valoración de la proporcionalidad en la determinación de la medida consistente en el tratamiento de los datos biométricos, sin que las autoridades de protección de datos puedan entrar a valorar la concurrencia de la proporcionalidad en el tratamiento, una vez la norma ha sido aprobada.

Siguiendo la doctrina emanada por el Tribunal Constitucional, el cumplimiento del principio de proporcionalidad exigirá superar los principios de idoneidad, necesidad y proporcionalidad. Así, señala la Sentencia del Tribunal Constitucional 207/1996 que se trata de “una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad”, añadiendo que “en este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que

no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)»

No existiendo duda alguna de que el tratamiento de los datos biométricos resulta idóneo para alcanzar las finalidades de control perseguidas, el problema estribará, precisamente en si en el supuesto planteado será posible alcanzar la finalidad perseguida a través de medios menos intrusivos en la esfera íntima del afectado con similar eficacia y si el uso de esta medida depara un mayor beneficio al interés general que el perjuicio que eventualmente pueda ocasionarse al afectado. Ello irá, como se ha reiterado, vinculado al grado de necesidad de realización del tratamiento para el mantenimiento de la relación jurídica en que pretende justificarse el mismo con arreglo al artículo 6.2 de la Ley Orgánica 15/1999 o el interés legítimo establecido en el artículo 7 f) de la Directiva 95/46/CE.

Pues bien, la solución que haya de darse al juicio de proporcionalidad y necesidad, necesario para considerar que el tratamiento respeta lo dispuesto en el artículo 4.1 de la Ley Orgánica 15/1999 y se encuentra legitimado por el artículo 6.2 de la misma o en el artículo 7 f) de la Directiva, no podrá ser única, debiendo en cada caso atender a la concreta finalidad perseguida, esto es, a la relación jurídica subyacente al tratamiento, a la situación del afectado y a las consecuencias que pudieran derivarse de la adopción de una medida menos gravosa para la intimidad del interesado.

En resumidas cuentas, deberán eludirse en el análisis juicios genéricos que conduzcan a respuestas únicas que no atiendan a las circunstancias del caso, a partir, al menos, de los tres parámetros que acaban de indicarse.

De este modo, no resultaría acorde a un adecuado juicio de proporcionalidad partir de la consideración de que el tratamiento de los datos biométricos debe siempre considerarse contrario a la legislación de protección de datos, dado que de hecho el legislador lo permite en determinadas ocasiones, como ya se ha indicado en relación con los identificadores únicos.

Tampoco sería adecuado considerar que el tratamiento de esos datos debería considerarse contrario a los principios de protección de datos cuando se lleva a cabo con una finalidad de control de acceso, dado que existirán supuestos en los que la garantía de la seguridad necesaria para el acceso a dichas instalaciones justifique el uso de este tipo de datos.

Pero igualmente no resultaría acorde con una debida aplicación de las normas de protección de datos considerar que cualquier tratamiento que redunde en una más eficiente asignación de los recursos justifica la utilización de los datos biométricos para el adecuado control de las actividades que conlleven la utilización de esos recursos, dado que una extensión de esa teoría podría llevar a un tratamiento indiscriminado del dato, al amparo de garantizar una mayor eficiencia en el gasto.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

IV

En consecuencia, el juicio de necesidad y proporcionalidad deberá analizarse en cada caso concreto. Así lo pone de manifiesto el documento WP80 del Grupo del artículo 29, cuando se refiere a estos casos, señalando que:

> *"El uso de la biometría plantea también el tema de la proporcionalidad de cada categoría de datos a la luz de los fines para los que se tratan dichos datos. Los datos biométricos sólo pueden usarse de manera adecuada, pertinente y no excesiva, lo cual supone una estricta valoración de la necesidad y proporcionalidad de los datos tratados. Por ejemplo, la CNIL francesa ha rechazado el uso de huellas digitales en el caso del acceso de los niños a un comedor escolar, pero ha aceptado con el mismo fin el uso de los resultados de muestras de las manos. La autoridad portuguesa de protección de datos ha tomado recientemente una decisión desfavorable sobre la utilización de un sistema biométrico (huellas digitales) por parte de una universidad para controlar la asiduidad y puntualidad del personal no docente."*

Tomando en cuenta este hecho, la Agencia Española de Protección de Datos ha atendido las distintas consultas que le han sido planteadas sobre esta cuestión, considerando la procedencia o improcedencia, en particular, del tratamiento de la huella dactilar en virtud de las circunstancias de cada caso concreto.

Así, en reiteradas ocasiones, se ha considerado conforme a la Ley Orgánica 15/1999 el tratamiento del citado dato para controlar el cumplimiento por los trabajadores o empleados públicos de su jornada laboral, a tenor de las circunstancias concurrentes en esta categoría de afectados y la dificultad de establecer otros procedimientos igual de eficientes e idóneos para garantizar el efectivo cumplimiento de las obligaciones derivadas del contrato de trabajo o de la relación estatutaria que vincula al funcionario con la Administración Pública. Así, en informe de 28 de febrero de 2006 se señalaba lo siguiente:

> *En efecto, en el ámbito de la relación jurídica que existe entre los trabajadores y el empresario al que prestan sus servicios, debe entenderse adecuado que éste recabe los datos que sean precisos para el normal desenvolvimiento de la misma y, dentro de estos datos, parece adecuado que se recaben del trabajador los necesarios para su identificación, a efectos de garantizar las medidas de seguridad que se consideren oportunas por parte de la empresa para que por la misma se pueda comprobar el grado de cumplimiento de las obligaciones que competen a los trabajadores.*

Ello no obstante, deberá darse cumplimiento a lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, dado que si bien no será preciso el consentimiento del interesado, si deberá advertirse al mismo de los extremos contenidos en ese precepto y, especialmente, de las consecuencias disciplinarias que podría acarrear su negativa a que la huella sea tratada.

Al propio tiempo, debe recordarse que los datos a los que se viene haciendo referencia podrían ser utilizados por el empresario única y exclusivamente para la función de control de la presencia del trabajador, tal y como se ha venido señalando, pero no para ninguna otra finalidad distinta, puesto que el artículo 4.2 de la Ley Orgánica 15/1999 dispone claramente que "Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos".

Además, en lo atinente a las medidas de seguridad en el tratamiento, debe señalarse que, teniendo en cuenta lo que se ha indicado en cuanto al dato biométrico de la huella digital, el mismo no puede ser considerado en modo alguno dato especialmente protegido o sensible, por lo que resultarán de aplicación al tratamiento las medidas de seguridad de nivel básico, previstas en el Reglamento de Seguridad, aprobado por Real Decreto 994/1999, de 11 de junio."

Sin embargo, y atendiendo al mismo juicio de proporcionalidad, el informe de 7 de septiembre de 2006, referido a una supuesto completamente distinto, señalaba que "*resulta desproporcionado y por ello contrario a lo dispuesto en el artículo 4.1 de la Ley Orgánica 15/1999 antes citado, la utilización de la huella dactilar como medio para controlar el acceso de los alumnos al centro escolar y tal finalidad puede conseguirse, sin duda, de una manera menos intrusiva en relación con los derechos de los alumnos*".

V

Por otra parte, no debe dejar de tenerse en cuenta, como ya se ha señalado, la exigencia del artículo 4.2 de la Ley Orgánica que, en el sentido derivado de la Sentencias del tribunal Constitucional 292/2000, de 30 de noviembre, impide el tratamiento de los datos para fines distintos de los que justificaron la recogida de los mismos. De este modo, la eventual proporcionalidad que pudiera encontrarse en el supuesto concreto quedaría completamente desvirtuada en caso de que los datos fueran empleados por el responsable para cualquier otra finalidad distinta de aquélla respecto de la que se considera posible el tratamiento. Esta cuestión es particularmente resaltada en el documento del Grupo del artículo 29, al recordar que "si la sociedad fomenta el desarrollo de bases de datos de huellas digitales u otras bases de datos biométricos para otras aplicaciones corrientes, se puede incrementar la reutilización potencial de esos datos por parte de otros como elemento de comparación e investigación en el marco de sus propios fines, sin haber pretendido inicialmente ese objetivo; las autoridades encargadas de hacer

cumplir la ley podrían figurar entre esos otros".

Al propio tiempo, y como recalca el documento WP80 debe tenerse en cuenta el ineludible cumplimiento de los deberes de información y seguridad previstos en las normas reguladoras del derecho fundamental a la protección de datos.

VI

Tomando en consideración lo que se ha venido indicando y el supuesto específicamente sometido al parecer de esta Agencia, consistente en el tratamiento de los datos de reconocimiento facial de los alumnos de los centros universitarios para el control de su asistencia a las clases y de su efectiva participación en las pruebas que se desarrollen en el centro, cabe considerar que el supuesto planteado se encuentra más próximo al relacionado con el uso de la huella digita para el control del acceso de los alumnos a un determinado centro escolar que con el control del cumplimiento de la jornada laboral por parte de los trabajadores, supuestos ambos ya analizados por la Agencia, en atención a la naturaleza del vínculo jurídico existente en uno y otro supuesto y la situación del colectivo afectado frente al responsable del fichero.

En este sentido, existen suficientes similitudes entre este supuesto y el ahora analizado que conllevan a considerar que la finalidad de control de asistencia podría lograrse igualmente a través de otros mecanismos, habitualmente utilizados hasta la fecha, que garanticen una mayor seguridad en el logro del objetivo sin necesidad de exigir el tratamiento del dato de la huella digital, sin que sea óbice para ello la mera afirmación de que dichos mecanismos son menos seguros que los que pretenden implantarse, por cuanto es posible el establecimiento de medidas más seguras de control que impidan la vulneración de los controles sin necesidad de por ello proceder al tratamiento de los datos de reconocimiento facial de los alumnos, con los consiguientes riesgos que ello pudiera aparejas.

Del mismo modo, a juicio de esta Agencia, el hecho de que la consultante considere que la medida ha sido acogida por los alumnos en relación con la prueba piloto realizada no supone en ningún caso que por ello quede legitimado el tratamiento de los datos, por cuanto, como ha venido indicándose dicho tratamiento vulnera, a nuestro juicio, el principio de proporcionalidad y, en segundo lugar, genera unos riesgos innecesarios derivados del propio tratamiento de los datos que no se concilian fácilmente con las normas reguladoras del derecho fundamental a la protección de datos de carácter personal.