AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Informe 0328/2012

I

La presente consulta versa sobre la implantación de un sistema de medición de audiencia, comercializado en España por la consultante, y su adecuación a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en adelante LOPD, y su normativa de desarrollo.

Según el escrito de consulta, el sistema se basa en la siguiente descripción: un sensor o dispositivo es instalado en pantallas digitales con emisión de contenidos publicitarios; puede captar imágenes sin grabarlas, de forma que una vez captada la imagen, es transferida al procesador que a través de un mecanismo de detección facial identifica las caras y las clasifica según género y edad. Al almacén de la memoria interna se transfieren datos relativos a un identificador de seguimiento, horas de aparición y desaparición de la persona, género y grupo de edad y periodos de tiempo en los que ha estado mirando. La información es remitida a un servidor de forma encriptada a efectos de realizar estudios de análisis de audiencias.

Y la consulta cuestiona si es de aplicación la normativa sobre protección de datos de carácter personal, si tiene que ver con ello el hecho de que las imágenes sufran una disociación irreversible, si es determinante para ello la capacidad de grabación y/o etiquetado de rostros, aunque el sistema de grabación esté desactivado; si existen diferentes criterios en función de la ubicación de los dispositivos, según se realice en espacios públicos exteriores, como la calle, o cerrados, como centros comerciales, tiendas o locales de ocio; y en caso de ser aplicable la LOPD, cuáles serían los requisitos legales para la implantación del sistema.

A efectos de protección de datos, entendemos que deben distinguirse dos fases o tratamientos diferenciados: un primer momento de captación de la imagen y tratamiento de la misma – es decir, englobando todo el proceso de detección facial y clasificación – y un segundo momento en el que la imagen ha desaparecido y se trata información no gráfica, incluyendo ciertos datos relativos a la identificación del seguimiento, hora de aparición y desaparición de la persona, periodos de tiempo en los que ha estado mirando, género y grupo de edad.

Entendemos que las conclusiones pueden ser distintas en ambos supuestos. En los dos casos debemos determinar si es de aplicación o no la legislación sobre protección de datos, como es sabido, la LOPD tiene por objeto, según su artículo 1, "*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". Es por ello que, según el artículo 2, el ámbito de aplicación viene referido a *"los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado"*. Y el artículo 3.a) LOPD define los datos de carácter personal como *"cualquier información concerniente a personas físicas identificadas o identificables".*

En este mismo sentido, si bien de una forma más descriptiva, el artículo 5.1.f) del Reglamento de desarrollo de la LOPD aprobado por Real Decreto 1720/2007 de 21 de diciembre (en adelante, RDLOPD) los define como "*cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*".

Todo ello, como no podía ser de otro modo, en consonancia con la Directiva 95/46/CE de 24 de octubre de 1995 del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de daos personales y a la libre circulación de estos datos. Su artículo 2.a) define datos personales como "*toda información sobre una persona física identificada o identificable (en "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.*"

Además, consideramos interesante mencionar la Opinión 3/2012 de 27 de abril de 2012 del Grupo de Trabajo creado al amparo del artículo 29 de la Directiva 95/46/CE sobre el desarrollo de las tecnologías biométricas. El supuesto de hecho planteado, en el que se trata la imagen de una persona a través de técnicas de reconocimiento facial con fines de análisis de audiencias de la publicidad sería una de las técnicas basadas en el comportamiento, en los términos del Documento de trabajo sobre biometría adoptado por el mismo Grupo de Trabajo el 1 de agosto de 2003 (WP80). La Opinión 3/2012 mencionada supone una importante guía para la interpretación de las normas sobre protección de datos en lo que a biometría se refiere.

II

En la primera fase del proceso indicado en la consulta, en la que un dispositivo o sensor capta una imagen y la trata, nos encontramos indudablemente ante un tratamiento de datos de carácter personal. La imagen de una persona es indudablemente un dato de carácter personal, conforme a la definición legal y reglamentaria antes expuesta, que incluye la información gráfica. Y por tratamiento entendemos, según el artículo 3.c) LOPD, "*operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".*

Así ha sido reiterado por esta Agencia en numerosísimas ocasiones, existiendo incluso una Instrucción relativa al tratamiento de imágenes a los fines de seguridad. Nos referimos a la Instrucción 1/1996 de esta Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras; dicha Instrucción no será de aplicación al supuesto de hecho planteado, puesto que la finalidad de la obtención de imágenes es totalmente distinta, si bien los criterios para el tratamiento de datos personales sí son los mismos.

En definitiva, siempre que exista un tratamiento de datos personales, como es la mera captación de imágenes, deberá darse cumplimiento a la LOPD y su normativa de desarrollo.

Comenzando por los **principios aplicables**, el artículo 4 LOPD en sus apartados 1 y 2 señala: *"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. 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. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos"*.

Resaltamos, por un lado, el principio de finalidad de los datos, de modo que los datos se recogen para una finalidad sin que puedan destinarse a otra diferente. Así, si se han obtenido para una finalidad lícita y explícita, como es la medición de audiencias - y no la del uso de la imagen para ofrecer, según género y edad, un tipo de publicidad u otra, que en palabras del Grupo de Trabajo del Artículo 29, sería de una categorización o segregación biométrica -, no podrán destinarse a ninguna otra finalidad diferente. En la medida en que el sistema sólo permita la captación de imágenes y mientras se mantenga el sistema de procesamiento expuesto en el escrito de consulta, la finalidad podría mantenerse. En este sentido, reiteramos que tanto para el cumplimiento del principio de finalidad como para la ponderación de la proporcionalidad que posteriormente veremos, es necesario partir del modelo de no grabación de imágenes ni conservación de las mismas más allá del tiempo imprescindible para su procesamiento mediante el reconocimiento facial. Sería imposible, por tanto, que si una persona ha sido captada, tratada su imagen y eliminada la misma - conservándose únicamente los parámetros indicados más arriba - y en un momento posterior la misma persona vuelve a aparecer, que el sistema propuesto permitiera asociar ambos momentos; es decir, si la imagen y todos los elementos que permitían identificar una persona han sido destruidos, la persona no será reconocible en el futuro, una vez procesada la imagen, aunque después vuelva a aparecer la misma persona ante el sensor.

Asimismo, esto implica que en ningún caso sea transferida la imagen –

de modo que esta sólo pueda permanecer en el procesador durante el brevísimo espacio de tiempo necesario para que dicho procesador realice su función – ni menos aún que la misma sea grabada o pueda serlo. Respondiendo así a la tercera pregunta del escrito de consulta, si bien entendemos que la mera captación de imágenes es ya un tratamiento de datos personales, exigiendo la aplicabilidad de la LOPD, si el sistema pudiera grabar, aunque fuera en potencia, partiríamos de un supuesto totalmente diferente. Esta capacidad de grabar, aunque el sistema de grabación no estuviera activado, influiría especialmente en la ponderación del juicio de proporcionalidad que posteriormente expondremos, puesto que la mera aptitud del sistema para conservar imágenes supondría un mecanismo mucho más intrusivo en el derecho fundamental a la protección de datos personales. En este caso los riesgos para la protección de datos serían mucho mayores, puesto que la conservación de las imágenes y su eventual uso posterior, para el mismo fin o relacionados, puede implicar serios perjuicios para las personas. Además, claro está, de ulteriores obligaciones legales.

En este mismo sentido la Opinión 3/2012 que antes mencionábamos, al afirmar – su texto aún se encuentra disponible sólo en inglés -: *"The Working Party warns of the risks involved in the use of biometric data for identification purposes in large centralised databases, given the potentially harmful consequences for the persons concerned".*

Y es que entre los riesgos del uso de datos biométricos esta Opinión habla del uso de los datos para fines distintos de los que fueron obtenidos; riesgo que, obviamente, concurriría si cupiera la grabación y/o almacenamiento de imágenes. Afirma el Grupo de Trabajo del artículo 29: *"The second risk is the purpose diversion either by the data controller itself or by a third-party including law enforcement authorities. This common threat regarding personal data becomes a crucial one when biometric data are used. Manufacturers should take all security measures to avoid any improper use of the data and make sure that any data that are not needed anymore for the purpose of the processing are deleted immediately.*
As with any other data, legitimately processed or stored biometric data or the sources of biometric may not be processed or enrolled by the controller for any new or other purpose unless there is a new legitimate ground for this new processing of these data".

Por tanto, las conclusiones de este informe sólo son aplicables en la medida en que el sistema no pueda grabar imágenes, aunque el sistema de grabación y/o almacenamiento esté desactivado, considerando que un sistema de grabación podría no cumplir los requisitos de proporcionalidad que posteriormente veremos; y que la imagen sea eliminada tan pronto como haya sido procesada.

Debe también recordarse, continuando con este punto, que los datos de datos de carácter personal deben conservarse exclusivamente durante el tiempo oportuno en función de la finalidad que justifique su tratamiento, en este caso los segundos necesarios para que la imagen sea procesada en los términos indicados; a este respecto dispone el artículo 4 de la LOPD que "*Los datos de carácter personal serán cancelados cuando hayan dejado de ser*

necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados."

También aquí la Opinión 3/2012 habla de la conservación de los datos biométricos durante el tiempo estrictamente necesario para el procesamiento de la misma, debiendo destruirse inmediatamente tras su utilización.

Junto con el principio de finalidad y conservación, hemos de destacar el principio de proporcionalidad. Como es sabido, la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina 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*".

En este sentido, esta Agencia ha destacado reiteradamente 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 expuestos por el Tribunal Constitucional: *"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)".*

En el supuesto de hecho consultado, la captación de imágenes – siempre que no exista grabación – parece que cumple el objetivo propuesto de medición de audiencias. También parece ser favorable el juicio de necesidad, desde un punto de vista de conveniencia y eficacia de costes. En cuanto al juicio de proporcionalidad en sentido estricto, siempre que la captación de imágenes se realice y se mantuviera durante el brevísimo espacio de tiempo necesario para que el procesador pueda realizar las funciones de disociación expuestas, podríamos considerar en algunos supuestos que es ponderada y equilibrada, teniendo siempre en cuenta que, en lo posible, se utilizarán medidas lo menos restrictivas posibles en la privacidad que pudieran lograr el objetivo propuesto.

Así, en espacios públicos cerrados tales como centros comerciales, tiendas o locales de ocio, en los que su actividad comercial pudiera

relacionarse íntimamente con la actividad publicitaria en la que se colocan los dispositivos, y por tanto la medición de audiencias puede resultar importante, la ponderación entre el perjuicio causado a los particulares y el beneficio para el que adopta la medida puede ceder a favor de este último. En este sentido, las personas que acceden a un centro comercial o a una tienda, o incluso a locales de ocio donde existen sistemas publicitarios, pueden razonablemente considerar que van a recibir publicidad y que el impacto de la misma va a ser medido.

Ahora bien, si tales dispositivos se situaran en la calle, en parques públicos, o en otros espacios abiertos o exteriores, el perjuicio para las personas iría en aumento, considerando que en cualquier momento y lugar podrían ser visionadas. Máxime teniendo en cuenta las importantes restricciones que para el ámbito de la seguridad pública existen en lo que a instalación de cámaras se refiere, estando esta materia absolutamente reservada a las Fuerzas y Cuerpos de Seguridad en los términos de la Ley Orgánica 4/1997 de 4 de agosto por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad Ciudadana en lugares públicos. Incluso teniendo en cuenta que, si bien las obligaciones de información del artículo 5 LOPD que posteriormente veremos podrían ser cumplidas cuando de espacios públicos cerrados se tratara, colocando un cartel informativo en un lugar visible, dicho deber de información sería de muy difícil cumplimiento en espacios públicos abiertos, en los que frecuentemente no hay puntos de entrada y salida concretos. Las personas difícilmente podrían ser informadas con carácter previo a la captación de su imagen en lugares públicos. En definitiva, cuando de espacios públicos abiertos se trata, entendemos que el perjuicio para el interés general y para el interés particular de las personas cuyas imágenes son captadas es superior al beneficio obtenido por la empresa consultante, por lo que en este punto la medida no sería ponderada.

En muy parecido sentido ha razonado la opinión 3/2012 la cautela que ha de adoptarse cuando de espacios públicos abiertos se trata, en los siguientes términos, referidos precisamente a técnicas de reconocimiento facial; y de nuevo aquí incide en que el juicio de proporcionalidad será mucho más favorable cuando no existe capacidad de grabación: *"In the case of facial recognition where biometric data can be easily captured without the knowledge of the data subject a widespread use would terminate anonymity in public spaces and allow consistent tracking of individuals. (…) A categorisation system to count demographics of visitors to an attraction with no recording capabilities will have a different impact on data protection to that from a system used for covert surveillance by law enforcement to identify potential troublemakers.*

Tracking / Profiling: An identification system could also be used if there is no knowledge of the real-world identity of an individual. A facial recognition system within a shopping centre or similar public area could be used to track routes and habits of individual shoppers. Purposes could be for effective queue management or product placement in order to improve the customer experience. However, with the ability to track or locate a specific individual

comes the ability to profile and deliver targeted advertising or other specific services".

En lo que atañe a la **legitimación**, el artículo 6.1 de la Ley Orgánica 15/1999 dispone que "*El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa".* Este consentimiento deberá ser, conforme a lo dispuesto en el artículo 3 h) *"libre, inequívoco, específico e informado".* El apartado segundo del artículo 6 introduce excepciones a la prestación del consentimiento. Ahora bien, tras la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, así como de las Sentencias del Tribunal Supremo de 8 de febrero de 2012 por las que se anula el apartado b) del artículo 10.2 RDLOPD, debemos considerar como otro supuesto legitimador la concurrencia del interés legítimo del que trata datos personales. La citada STJUE de 24 de noviembre de 2012 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.

Así pues, la **Sección 1ª de la Sala de lo Contencioso Administrativo de la Audiencia Nacional** viene realizando una ponderación caso por caso de la relación entre el interés legítimo y los derechos y libertades fundamentales del interesado. Así, la primera resolución que trató la cuestión fue la de **15 de marzo de 2012** dictada en el recurso 390/2010; respecto de la ponderación señalaba que "*Ponderación de intereses en conflicto que dependerá de las circunstancias concretas de cada caso y en la que no obstante, sí puede tomarse en consideración, a efectos de determinar la posible lesión de los derechos fundamentales del afectado, el hecho de que los datos figuren ya, o no, en fuentes accesibles al público. Más ello, simplemente, como un elemento más de ponderación".*

Y en ese caso concreto, relativo al tratamiento de datos relativos del libro genealógico de la cría de caballos de pura raza española, apreció que el interés legítimo del responsable del tratamiento debía prevalecer porque *"Nos hallamos, por tanto, ante unos datos personales extraídos de un sitio virtual, de acceso público, y que se exponen en la página web titularidad de la entidad actora (según resulta de las actuaciones) con la finalidad de dar información estadística sobre el caballo de pura raza española y posibilitar un rápido acceso a dicha información, sobretodo facilitar el cruce o comparación de datos entre todos los registros.*

Consideramos, por todo ello, que existen intereses legítimos de tal titular de la pagina web, e incluso intereses de terceros (de los propietarios o criadores de caballos) en acceder a dicha información publicada en Internet, intereses que se estiman prevalentes respecto del derecho a la protección de datos de los afectados por dicha información, y que por tanto excluyen la necesidad de consentimiento de los mismos".

En parecido sentido la **Sentencia de 31 de mayo de 2012**, PO 793/2010, apreció el interés legítimo del miembro de un colegio oficial y una asociación para el tratamiento de datos de los integrantes del cuerpo electoral, puesto que se presentaba a las elecciones internas de dicho colegio oficial. Si bien en este supuesto existía también el consentimiento de los titulares de los datos personales.

La **Sentencia de 6 de junio de 2012**, PO 594/2009, apreció que el interés legítimo del responsable del fichero no debía prevalecer, en la ponderación, sobre la protección de datos personales, en los siguientes términos: *"La Sala, a la vista de las circunstancias concurrentes expuestas, considera que debe prevalecer el derecho a la protección de datos de los denunciantes afectados incluidos en el citado fichero Domicilios, frente a los intereses particulares de la recurrente en explotar la citada base de datos que contiene nada menos que 37.000.000 de registros de datos personales, con la información asociada a los mismos ya indicada y recogida de la forma expuesta.*

En efecto, no es lo mismo que una determinada empresa necesite averiguar el domicilio de una persona de la que es acreedora, a efectos de poder efectuar el cobro de la deuda (para lo cual y a efectos de satisfacer ese interés legítimo puede utilizar los medios adecuados y lícitos tendentes a averiguar ese nuevo domicilio y poder tratarlo en orden a dicha finalidad), que el hecho de la creación de un mega fichero como el que nos ocupa (que se reitera contiene 37.000.000 de registros de datos personales), con el fin de poder comercializarlo y ofrecer esa información obtenida. Además, como también se ha expuesto en algunos casos la información se asocia o abarca a las personas que conviven en el mismo domicilio que la que aparece registrada en el fichero, lo que conculca el derecho de protección de datos de los afectados

Por tanto, debe concluirse que no concurre el interés legítimo alegado por la entidad recurrente (que obviamente no es la persona física o jurídica que puede tener interés en el cobro de las posibles deudas) para tratar y, en correlación, ceder dichos datos de carácter personal, debiendo prevalecer el derecho de los afectados a la protección de datos, por lo que deben entenderse cometidas las infracciones apreciadas por la resolución impugnada".

En el supuesto de hecho planteado, entendemos que el consultante puede tener un interés legítimo en realizar un seguimiento de las campañas publicitarias mediante análisis de audiencias o técnicas similares. En el otro lado encontramos la protección de derechos o libertades fundamentales, que en este caso identificamos con el derecho al *habeas data*, al control sobre los propios datos de carácter personal como son la imagen de una persona. Ahora bien, en la ponderación concreta entre ambos encontramos que el justo

equilibrio al que se refiere la jurisprudencia comunitaria podemos encontrarlo en el lugar de ubicación de los dispositivos en cuestión, como antes mencionábamos al estudiar el principio de proporcionalidad. Si bien el interés legítimo puede prevalecer en el caso de espacios públicos cerrados, precisamente destinados a fines comerciales, en la medida en que – siempre suficientemente informados, como posteriormente veremos – los que acuden pueden razonablemente aceptar que recibirán publicidad con la consiguiente medición de audiencia de la publicidad, no así en espacios públicos abiertos, en los que quedaría totalmente fuera de su poder de disposición la utilización de los datos.

III

En los términos expuestos en los que una medida podría considerarse ponderada y con legitimación suficiente, la implantación del sistema requeriría el cumplimiento de todas las obligaciones de la LOPD.

En primer lugar, al tratarse en esta primera fase datos de carácter personal, deberá cumplirse el deber de **información** al afectado, exigido en el artículo 5 de la LOPD, conforme al cual *"Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*

a. De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b. Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c. De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e. De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante."

Existen una serie de obligaciones legales que en el supuesto de hecho planteado, podrían no ser de aplicación, en la medida en que no exista grabación, ni siquiera en potencia. Así, si bien teóricamente habrían de garantizarse el ejercicio de los **derechos de acceso, rectificación, oposición y cancelación** de los artículos 13 y ss. LOPD, en la práctica no podrían atenderse. Lo mismo sucede con la **cesión** a terceros que debe cumplir los requisitos legales establecidos en el art. 11 LOPD y 10 del Real Decreto 1720/2007 por el que se aprueba el Reglamento de la LOPD (en adelante, RDLOPD). Además, el responsable del fichero y, si lo hubiera, el encargado del tratamiento (regulado en el art. 12 LOPD y 20 RDLOPD) deberán adoptar, de conformidad con el art. 9 LOPD, "*las medidas de índole técnica y organizativas necesarias que garantice la seguridad de los datos de carácter personal y evite su alteración, pérdida, tratamiento o acceso no autorizado*". Las **medidas de seguridad** aparecen desarrolladas en el Título VIII, arts. 79 y ss. del RDLOPD, y dependerán de los datos que se hagan constar en el tratamiento, de conformidad con el art. 81, y son de aplicación a todo tratamiento de datos

personales, aunque no exista grabación de imágenes. Serán exigibles aquellas que sean de aplicación al supuesto de hecho, teniendo en cuenta el artículo 87 relativo a los ficheros temporales. A efectos interpretativos puede ser interesante de nuevo la Opinión 3/2012 mencionada – disponible en la dirección http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion- recommendation/files/2012/wp193_en.pdf, que precisamente hace alusión a medidas de seguridad concretas que deberían adaptarse en estos casos (especialmente el punto 5.4.1), haciendo especial incapié en varias ocasiones en los sistemas de protección anti-spoofing y a la implantación de sistemas que automáticamente eliminen todo tipo de datos de carácter personal. También se mencionan medidas de índole organizativa, como la instrumentación de procesos que aseguren que sólo tendrán acceso a datos personales los usuarios habilitados como tales, con seguimiento de todas las actuaciones; incluso se refiere a la subcontratación de estos servicios, aplicándose la figura del encargado del tratamiento en este caso (art. 12 LOPD).

IV

Para el estudio de la segunda fase del proceso indicado debemos volver a los conceptos expuestos en el apartado I del presente informe. Es decir, para el análisis de la aplicabilidad de la legislación sobre protección de datos deberá estarse a la capacidad de identificar a la persona a la que se refieren los datos. En definitiva, no tiene por qué ser una persona identificada, bastará que sea identificable por medios que no resulten desproporcionados. Así, en esta segunda fase existe un primer problema con la determinación del concepto "identificador de seguimiento". Si esto se refiere a la asignación de un número a una persona concreta, y que en caso de repetirse el rostro se le asignaría el mismo número, entendemos que sí se están tratando datos de carácter personal. Ahora bien, si como parece ofrecerse en la descripción del sistema, la imagen es destruida de forma absoluta, con carácter irreversible, y por tanto el identificador no estaría asociado a una imagen, de forma que sólo supondría la asignación de una numeración dentro del sistema, el mismo no puede configurarse como dato de carácter personal. Los otros dos elementos que podrían determinar que esta fase implicara el tratamiento de datos personales podrían ser el género y el grupo de edad, puesto que los demás – horas de aparición y desaparición de la persona y periodos de tiempo que ha estado mirando – no permiten, por sí mismos, identificar a una persona. Si existieran otros datos que permitieran identificar a las personas, estos otros accesorios sí se convertirían en datos personales, puesto que ofrecen información sobre personas físicas identificadas o identificables. Ahora bien, por sí mismos e individualmente considerados no permiten identificar personas.

En cuanto al género y grupo de edad, entendemos que el género por sí mismo no permite identificar a nadie en concreto; y en la medida en que el grupo de edad sea suficientemente amplio – niño, adulto, senior, o categorías similares – tampoco es por sí mismo ni en conjunción con los restantes datos

que se mencionan en la petición de informe, suficiente para determinar que una persona sea identificable. Es decir, en la medida que los datos obtenidos por el sistema no ofrezcan, aislada o conjuntamente considerados, elementos suficientes para que podamos afirmar que se trata de personas identificables, no nos encontramos en esta segunda fase ante datos de carácter personal, y por tanto no es de aplicación la normativa sobre protección de datos de carácter personal.

Ahora bien, respondiendo a la segunda pregunta postulada, reiteramos que para que en esta segunda fase no se aplique la normativa de protección de datos es necesario que no se esté tratando ningún dato de carácter personal, que permita identificar a una persona, incluida su imagen. Así pues, sólo en la medida en que en esta segunda fase las personas no sean identificables, de forma que los datos se hayan disociado completamente, no será de aplicación la LOPD. En este sentido, el artículo 5.1.e) RDLOPD define dato disociado como "*aquél que no permite la identificación de un afectado o interesado*".

En este sentido volvemos de nuevo a la Opinión 3/2012 de 27 de abril de 2012 del Grupo de Trabajo creado al amparo del artículo 29 de la Directiva 95/46/CE sobre el desarrollo de las tecnologías biométricas. Nos encontraríamos ante técnicas basadas en el comportamiento, en los términos del Documento de trabajo sobre biometría adoptado por el mismo Grupo de Trabajo el 1 de agosto de 2003 (WP80). Se habla así de *"**Biometric template**: Key features can be extracted from the raw form of biometric data (e.g. facial measurements from an image) and stored for later processing rather than the raw data itself. This forms the biometric template of the data. The definition of the size (the quantity of information) of the template is a crucial issue. On the one hand, the size of the template should be wide enough to manage security (avoiding overlaps between different biometric data, or identity substitutions), on the other hand, the size of the template should not be too large so as to avoid the risks of biometric data reconstruction. The generation of the template should be a one-way process, in that it should not be possible to regenerate the raw biometric data from the template".*

En este punto, consideramos importante destacar que la única información que se almacena, con carácter irreversible, es la indicada en el escrito de consulta que, sirviendo para realizar los análisis de audiencias, no contenga ningún elemento que permita identificar, ni siquiera mediante esfuerzos desproporcionados en este caso, a una persona. Sólo así entendemos que se cumplen los principios expuestos en el presente informe.