



La consulta solicita un informe vinculante sobre la adecuación a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, del sistema de videovigilancia descrito en la consulta.

I

Con carácter previo, debe señalarse que, si bien dentro de las competencias atribuidas a esta Agencia de Protección de Datos se encuentra, según establece el artículo 37.1.e) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, la de *“proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal”*, en modo alguno tal atribución puede considerarse que lleva aparejada la competencia para dictar informes con efecto vinculante.

Por otra parte, debe tenerse en cuenta que a partir del 25 de mayo de 2018 resultarán de aplicación las disposiciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Dicho Reglamento sustituirá la normativa que hasta ahora venía rigiendo la materia, esto es, la Directiva 95/46 CE y la normativa que en cada país la desarrolla, normativa que en España viene constituida fundamentalmente por 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. De este modo, debe examinarse el supuesto objeto de consulta teniendo en cuenta ambas normativas, puesto que la solución puede ser diferente bajo una u otra.

II

En lo que respecta a la normativa actualmente aplicable, debe indicarse que los artículos 1 y 2 de la Ley Orgánica 15/1999, extienden su protección a



los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos de carácter personal, siendo definidos éstos en el artículo 3.a) de la citada Ley como *“cualquier información concerniente a personas físicas identificadas o identificables.”*

Por su parte, el artículo 5.1.f) del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, precisa que constituye un dato de carácter personal *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.”*

Dichas definiciones se encuentran, como no podría 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 datos personales y a la libre circulación de estos datos, cuyo artículo 2.a) define los datos personales como *“toda información sobre una persona física identificada o identificable (el “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.”*

De este modo, la imagen de una persona identificada o identificable constituye un dato de carácter personal. En lo que respecta a la plantilla biométrica de las caras que se pretende crear cabe recordar que el Grupo de Trabajo del artículo 29, órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE, en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas recordaba que, en anteriores Dictámenes, se habían definido los datos biométricos como *“propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad”*. Señala dicho dictamen que a veces la información biométrica capturada de una persona se almacena y se trata en bruto, lo que permite reconocer la fuente de la que procede sin conocimientos especiales; por ejemplo, la fotografía de una cara, la fotografía de una huella dactilar o una grabación de voz. Otras veces, la información biométrica bruta capturada es tratada de manera que solo se extraen ciertas características o rasgos y se salvan como una plantilla biométrica.



En lo que se refiere a las plantillas biométricas, el aludido Grupo de Trabajo del artículo 29, en su Dictamen 02/2012 sobre reconocimiento facial en los servicios en línea y móviles, señalaba igualmente que *“Por definición, una plantilla creada a partir de una imagen de una persona también es un dato personal desde el momento en que contiene un conjunto de características distintivas de su rostro que se asocian a una persona concreta y se almacenan como referencia para comparaciones futuras en procesos de identificación y autenticación/verificación.”*

De este modo, el patrón de la cara de las personas, o lo que es lo mismo, la plantilla biométrica tendrá el carácter de dato personal conforme a la definición de éste contenida en los artículos 3.a) de la Ley Orgánica 15/1999 y 5.1.f) de su Reglamento de desarrollo, en tanto contiene un conjunto de características distintivas de cada una de ellas suficientes para identificarle y diferenciarle de otras personas de forma que pueda reconocérsele en cada visita que efectúe al establecimiento, por lo que dicha información está indudablemente asociada a una persona identificada o identificable.

El requisito capital para que un tratamiento de datos personales sea conforme a la Ley Orgánica 15/1999 es que su responsable se encuentre legitimado para efectuar el mismo. Cuando no se trata de datos especialmente protegidos, el artículo 6.1 de dicha Ley exige el consentimiento inequívoco del afectado salvo que la Ley disponga otra cosa. El apartado segundo de dicho artículo 6 introduce determinadas excepciones a la necesidad de consentimiento, que no resultan de aplicación al presente supuesto, a las que debe añadirse la prevista en el artículo 7.f de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, cuyo efecto directo ha sido declarado expresamente por la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, 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”*.



Debe, por ello, examinarse si el tratamiento de datos objeto de consulta podría venir legitimado en lo previsto en el artículo 7.f de la Directiva 95/46/CE. En este sentido, 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 que, conforme a su apartado 47 *“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 que prevalezca sobre el interés o los derechos y libertades fundamentales de los 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 afectados por el tratamiento de los datos de carácter personal han de prevalecer sobre el interés legítimo en que el responsable pretende fundamentar dicho tratamiento.



Esta Agencia ha examinado en diversas ocasiones la legitimación para llevar a cabo el tratamiento de datos con fines de videovigilancia, considerando que existe un interés legítimo en la captación de imágenes por parte de particulares mediante cámaras de videovigilancia para garantizar la seguridad de personas o bienes en los espacios de su propiedad dentro de un edificio o, en su caso, en cuya legítima posesión se encuentren, considerando igualmente que tal interés prevalecerá sobre los derechos de los afectados cuando tal tratamiento sea proporcional y vinculado al principio de finalidad.

Ahora bien, en el presente supuesto no solamente se captan imágenes para detectar ilícitos y poner las mismas a disposición de la policía o los órganos judiciales, sino que se identifica al presunto infractor guardando una plantilla biométrica que permite al sistema de videovigilancia la detección de dicha persona cuando entra de nuevo en el centro comercial y avisa de su entrada al personal de seguridad o al personal del centro.

En este sentido el Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara, señalaba que *“Las tendencias relativas a la evolución de las técnicas de vigilancia por videocámara podrían evaluarse de manera provechosa para evitar que el desarrollo de aplicaciones informáticas basadas tanto en el reconocimiento fisonómico como en el estudio y el pronóstico del comportamiento humano reproducido conduzca de manera involuntaria a una vigilancia dinámico preventiva, en contraposición con la vigilancia estática convencional, cuyo objetivo suele ser la documentación de acontecimientos específicos y de sus autores. Esta nueva forma de vigilancia está basada en la captación automatizada de los rasgos faciales de personas físicas y de su conducta «anormal» asociada a la disponibilidad de señales y avisos automatizados, lo que probablemente acarree riesgos de discriminación.”*

Teniendo en cuenta que esta finalidad adicional de generar una plantilla biométrica de quien presuntamente ha cometido un robo en un centro comercial, a fin de detectar nuevamente su entrada en el mismo y dar avisos al personal para que sea sometido a una vigilancia física específica, comporta un mayor riesgo para los derechos y libertades de las personas que los sistemas tradicionales que se limitan a captar la comisión del presunto ilícito debe ponderarse si tal finalidad adicional puede prevalecer sobre los derechos y libertades fundamentales de las personas.



A estos efectos, esta Agencia ha valorado en diversas ocasiones la aportación de garantías que permitan considerar que el perjuicio de los derechos de los interesados se verá disminuido para poder entender prevalente el interés legítimo aducido sobre el eventual riesgo producido como consecuencia del tratamiento de datos pretendido.

Tales garantías pueden consistir en el refuerzo de los principios y obligaciones contenidos en la normativa de protección de datos, pudiendo señalarse las siguientes a título orientativo y sin perjuicio de que por el consultante se añadan mayores garantías.

En lo que respecta a la intensificación de los principios de calidad consagrados en el artículo 4 de la Ley Orgánica 15/1999, debe aquí hacerse referencia, en primer lugar, a los principios de proporcionalidad y finalidad recogidos en los números 1 y 2 de dicho artículo respectivamente. Dispone el artículo 4.1 que *“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.”* El número 2 de dicho precepto establece 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. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.”*

Cabe recordar que la proporcionalidad exige, según la doctrina del Tribunal Constitucional, siguiendo a tal efecto la sentada por el Tribunal Europeo de Derechos Humanos, la superación de un triple juicio, en el sentido de determinar si la medida adoptada 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), es decir, si la injerencia producida en el titular del derecho objeto de restricción por la medida es la mínima en aras al logro del fin legítimo perseguido con aquélla.

Así pues la creación de la plantilla solamente se encuentra justificada si persigue una finalidad determinada, explícita y legítima y, en tal caso, dicha



medida es idónea, necesaria y equilibrada o, en los términos, de la Ley Orgánica 15/1999, los datos a tratar son adecuados, pertinentes y no excesivos para la consecución de tal finalidad. De lo expuesto en la consulta se desprende que se pretende adoptar tal medida en aquellos supuestos en que se producen pequeños hurtos que según señala no tienen repercusión penal por ser de valor inferior a 400 euros, debe así tenerse en cuenta, en primer lugar que en el año 2015 se ha producido una reforma del Código Penal que atiende a tales situaciones, configurándolas no como falta, sino como delito, con la finalidad expresada en la propia ley de ofrecer respuesta a los problemas que plantea la multirreincidencia. No obstante, si aún pesar de dicha modificación cupiese justificar la proporcionalidad de la medida para evitar la comisión de tales delitos, lo que exige el examen de cada caso concreto, deberán extremarse las precauciones para que no se creen plantillas con motivo de la existencia de un falso positivo o en el caso de situaciones dudosas. En este sentido, la consulta solamente señala que no se trata de una detección automática, sino que se valida la comisión del acto por “persona autorizada”, sin que se aporten mayores precisiones. A juicio de esta Agencia, no solamente deberá ser posible probar mediante las imágenes que dicha persona ha cometido el delito, sino que debe procederse a la denuncia del mismo, en este sentido debe tenerse en cuenta que el Título I del libro II de la Ley de Enjuiciamiento Criminal (LECrim) en sus arts. 259, 262 y 264 establece diversos casos en que quien presencia la perpetración de un delito debe denunciarlo (esto es, comunicarlo) a la policía, fiscal o tribunales, bajo pena de multa.

Por otra parte el artículo 4.1 de la Ley Orgánica 15/1999 Ley exige que la finalidad del tratamiento sea “determinada, explícita y legítima”, del mismo modo exige en su artículo 5 que se informe a los interesados por el tratamiento de la finalidad de la recogida de los datos. De este modo dicha finalidad de generar una plantilla biométrica de quien presuntamente comete un ilícito para identificarle cuando se produce la entrada en el centro comercial, debe ser expresada en la información que se ofrezca, puesto que tal finalidad ni se contempla en el aviso que la consulta aporta, ni responde a las expectativas de las personas que entran en lugares objeto de videovigilancia, expectativas que se limitan a que tales imágenes se puedan utilizar como prueba de la comisión de delitos en los procesos penales, pero no de un tratamiento adicional del carácter del señalado en la consulta.

Asimismo, teniendo en cuenta que su finalidad es evitar la comisión en el centro comercial de los delitos a que la consulta hace referencia, será preciso

que el tratamiento del dato de la plantilla biométrica quede limitado al centro comercial del responsable del fichero, de modo que no se produzca una comunicación de tal dato a otros centros, generándose así una situación injustificada de estigmatización de las personas afectadas. Debe así recordarse que dicha comunicación de datos constituiría una cesión de datos definida en el artículo 3.i) de la Ley Orgánica 15/1999 como *“toda revelación de datos realizada a una persona distinta del interesado”*. Tal cesión deberá sujetarse al régimen general de comunicación de datos de carácter personal regulado en el artículo 11 de dicha ley, donde se establece que la misma solo puede verificarse para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y cesionario y exige para que pueda tener lugar, el consentimiento del interesado (artículo 11.1), otorgado con carácter previo a la cesión y suficientemente informado de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar (artículo 11.3), y que debe recabar el cedente como responsable del fichero que contiene los datos que se pretenden ceder.

Asimismo en lo que respecta al principio de exactitud, el número 3 del artículo 4 dispone que *“Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado”*. Ello exige que la plantilla biométrica debe poder relacionarse con las imágenes que muestran la comisión del delito, ya que esta es la justificación para tal tratamiento de datos, de modo que no se generen plantillas biométricas que respondan a otras motivaciones, sin embargo tal tratamiento no puede efectuarse indefinidamente en el tiempo, de modo que cabría considerar como una garantía el plazo de un mes que señala el consultante para la cancelación tanto de las imágenes como de la plantilla, cancelación que debe efectuarse de forma automática.

En lo que respecta a otras obligaciones impuestas por la normativa de protección de datos, deben resaltarse las relativas a los derechos de acceso, rectificación, cancelación y oposición. El consultante señala en este sentido que pueden ejercitarse tales derechos ante el centro comercial, de modo que en caso de ejercitarse el derecho de acceso deberá darse información de la existencia de una plantilla biométrica creada a partir de los rasgos faciales del interesado.

En cuanto a las medidas de seguridad, la consulta indica que se someterían a medidas de seguridad de nivel alto. A estos efectos cabe recordar

que tales medidas se regulan en el Reglamento de desarrollo de la ley Orgánica 15/1999 y tienen carácter acumulativo de forma que las establecidas para cada nivel exigen incorporar las previstas para los niveles inferiores, tal y como prevé el artículo 81 de dicha norma.

Por otra parte, no queda claro en la consulta quien es el responsable del fichero o tratamiento, ya que la finalidad de videovigilancia entendida como vigilancia estática en los términos del grupo de trabajo del 29 parece atribuirse a lo que la consulta denomina puntos de venta, pareciendo desprenderse de la misma que son los diferentes establecimientos situados en el recinto del centro comercial, mientras que atribuye la responsabilidad del tratamiento de la plantilla biométrica al centro comercial. No resulta así claro si se producen cesiones de datos entre los diversos responsables, o si la posición del centro comercial debe ser la propia de un encargado del tratamiento.

De este modo, clarificándose quién es el responsable del tratamiento y dando cumplimiento a las garantías señaladas, así como cualquier otra adicional que plantee el consultante, el interés legítimo del responsable podría prevalecer sobre los derechos fundamentales de los afectados por dicho tratamiento.

III

No obstante lo anteriormente señalado debe tenerse en cuenta que a partir de 25 de mayo de 2018 resultarán de aplicación al caso las disposiciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Dicha norma, como se ha señalado, constituirá la normativa aplicable sustituyendo a la normativa nacional actualmente de aplicación.

En lo que al presente supuesto respecta, debe tenerse en cuenta que el artículo 9 de dicho Reglamento incluye entre las categorías especiales de datos personales los “datos biométricos dirigidos a identificar de manera unívoca a una persona física”, estableciendo los supuestos en que cabe su tratamiento, de los que queda excluido el interés legítimo analizado anteriormente. Dispone el aludido artículo 9 lo siguiente:



“1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;



f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.”

Por consiguiente, aunque en la actualidad el tratamiento de la plantilla biométrica a que la consulta se refiere pudiese encontrarse legitimado en lo previsto en el artículo 7.f de la Directiva 95/46/CE en los términos antes vistos, a partir del 25 de mayo de 2018 tal tratamiento no podrá fundarse en dicho precepto, pasando a constituir un dato especialmente protegido cuyo



tratamiento solo será posible en los casos que permite el artículo 9 del Reglamento arriba transcrito, casos en los que no es posible el encaje de dicho tratamiento, de modo que sólo sería posible con el consentimiento del afectado por el tratamiento.