N/REF: 010308/2019

En el escrito de consulta se plantean, en esencia, dos cuestiones de carácter general: la primera, la posible exclusión de las actividades de seguridad privada, por tratarse de actividades subordinadas a la seguridad pública, del ámbito de aplicación 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, RGPD) conforme a su artículo 2.2, letra d) y la segunda, la licitud de la incorporación de sistemas de reconocimiento facial en los servicios de videovigilancia al amparo del artículo 42 de la Ley de Seguridad Privada.

I

La primera cuestión que se plantea en la consulta es la relativa a si, atendiendo a que las actividades de seguridad privada son actividades subordinadas a la seguridad pública, determinados tratamientos de datos efectuados por Empresas y Personal de seguridad privada pudieran encuadrarse, o no, en el artículo 2.2 letra d) del Reglamento general de protección de datos.

El carácter complementario de los servicios de seguridad privada y su subordinación a las Fuerzas y Cuerpos de Seguridad, de quien son colaboradoras, aparece reconocido, de manera reiterada, en la Ley 5/2014, de 4 de abril, de Seguridad Privada. En este sentido, su Exposición de Motivos destaca que “En la relación especial que mantiene la seguridad privada con las Fuerzas y Cuerpos de Seguridad, auténticos garantes del sistema de libertades y derechos que constitucionalmente protegen, se hace necesario avanzar en fórmulas jurídicas que reconozcan el papel auxiliar y especialmente colaborador desempeñado por la seguridad privada, de forma que, además de integrar funcionalmente sus capacidades en el sistema público de seguridad, les haga partícipes de la información que resulte necesaria para el mejor cumplimiento de sus deberes” y que “En resumen, puede decirse que el conjunto de los cambios propuestos en la nueva ley, además de mejorar y resolver problemas técnicos, de gestión y operativos, profundiza decididamente en el actual modelo español de seguridad privada (complementaria, subordinada, colaboradora y controlada por la seguridad pública), apostando por su papel preventivo en beneficio de la seguridad general, y lo hace

aprovechando e integrando funcionalmente todo su potencial informativo, de recursos humanos y de medios materiales, al servicio de la protección y seguridad del conjunto de la ciudadanía, de forma compatible con el legítimo interés que persiguen las entidades privadas de seguridad".

Partiendo de lo anterior, el artículo 1 define el objeto de la ley de la siguiente manera:

> 1. Esta ley tiene por objeto regular la realización y la prestación por personas privadas, físicas o jurídicas, de actividades y servicios de seguridad privada que, desarrollados por éstos, son contratados, voluntaria u obligatoriamente, por personas físicas o jurídicas, públicas o privadas, para la protección de personas y bienes. Igualmente regula las investigaciones privadas que se efectúen sobre aquéllas o éstos. Todas estas actividades tienen la consideración de complementarias y subordinadas respecto de la seguridad pública.
>
> 2. Asimismo, esta ley, en beneficio de la seguridad pública, establece el marco para la más eficiente coordinación de los servicios de seguridad privada con los de las Fuerzas y Cuerpos de Seguridad, de los que son complementarios.

Por su parte, el artículo 2 define la seguridad privada como "el conjunto de actividades, servicios, funciones y medidas de seguridad adoptadas, de forma voluntaria u obligatoria, por personas físicas o jurídicas, públicas o privadas, realizadas o prestados por empresas de seguridad, despachos de detectives privados y personal de seguridad privada para hacer frente a actos deliberados o riesgos accidentales, o para realizar averiguaciones sobre personas y bienes, con la finalidad de garantizar la seguridad de las personas, proteger su patrimonio y velar por el normal desarrollo de sus actividades".

Y el artículo 4, establece sus fines específicos:

La seguridad privada tiene como fines:

> a) Satisfacer las necesidades legítimas de seguridad o de información de los usuarios de seguridad privada, velando por la indemnidad o privacidad de las personas o bienes cuya seguridad o investigación se le encomiende frente a posibles vulneraciones de derechos, amenazas deliberadas y riesgos accidentales o derivados de la naturaleza.
>
> b) Contribuir a garantizar la seguridad pública, a prevenir infracciones y a aportar información a los procedimientos relacionados con sus actuaciones e investigaciones.
>
> c) Complementar el monopolio de la seguridad que corresponde al Estado, integrando funcionalmente sus medios y capacidades como un recurso externo de la seguridad pública.

Desarrollando dicho deber de colaboración, los artículos 14 y 15 de la Ley regulan las comunicaciones de datos que puedan realizarse entre las empresas de seguridad, despachos de detectives y el personal de seguridad privada y las Fuerzas y Cuerpos de Seguridad, que deberán respetar, en todo caso, lo establecido en la normativa de protección de datos de carácter personal:

> Artículo 14. Colaboración profesional.
>
> 1. La especial obligación de colaboración de las empresas de seguridad, los despachos de detectives y el personal de seguridad privada con las Fuerzas y Cuerpos de Seguridad se desarrollará con sujeción al principio de legalidad y se basará exclusivamente en la necesidad de asegurar el buen fin de las actuaciones tendentes a preservar la seguridad pública, garantizándose la debida reserva y confidencialidad cuando sea necesario.
>
> 2. Las empresas de seguridad, los despachos de detectives y el personal de seguridad privada deberán comunicar a las Fuerzas y Cuerpos de Seguridad competentes, tan pronto como sea posible, cualesquiera circunstancias o informaciones relevantes para la prevención, el mantenimiento o restablecimiento de la seguridad ciudadana, así como todo hecho delictivo del que tuviesen conocimiento en el ejercicio de su actividad o funciones, poniendo a su disposición a los presuntos delincuentes, así como los instrumentos, efectos y pruebas relacionadas con los mismos.
>
> 3. Las Fuerzas y Cuerpos de Seguridad podrán facilitar al personal de seguridad privada, en el ejercicio de sus funciones, informaciones que faciliten su evaluación de riesgos y consiguiente implementación de medidas de protección. Si estas informaciones contuvieran datos de carácter personal sólo podrán facilitarse en caso de peligro real para la seguridad pública o para evitar la comisión de infracciones penales.
>
> Artículo 15. Acceso a la información por las Fuerzas y Cuerpos de Seguridad.
>
> 1. Se autorizan las cesiones de datos que se consideren necesarias para contribuir a la salvaguarda de la seguridad ciudadana, así como el acceso por parte de las Fuerzas y Cuerpos de Seguridad a los sistemas instalados por las empresas de seguridad privada que permitan la comprobación de las informaciones en tiempo real cuando

ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

2. El tratamiento de datos de carácter personal, así como los ficheros, automatizados o no, creados para el cumplimiento de esta ley se someterán a lo dispuesto en la normativa de protección de datos de carácter personal.

3. La comunicación de buena fe de información a las Fuerzas y Cuerpos de Seguridad por las entidades y el personal de seguridad privada no constituirá vulneración de las restricciones sobre divulgación de información impuestas por vía contractual o por cualquier disposición legal, reglamentaria o administrativa, cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

Partiendo de dicha configuración de la seguridad privada en nuestro ordenamiento jurídico, la consulta plantea la posible aplicación de la exclusión establecida en el artículo 2.2.d) del RGPD, según el cual:

2. El presente Reglamento no se aplica al tratamiento de datos personales:

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención

Dicha exclusión se justifica como consecuencia de la existencia de un régimen específico aplicable a dicho tratamiento, tal y como señala el Considerando 19:

La protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención, es objeto de un acto jurídico específico a nivel de la Unión. El presente Reglamento no debe, por lo tanto, aplicarse a las actividades de tratamiento destinadas a tales fines. No obstante, los datos personales tratados por las autoridades públicas en aplicación del presente Reglamento deben, si se destinan a tales fines, regirse por un acto jurídico de la Unión más específico, concretamente la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo. Los Estados miembros pueden encomendar a las autoridades competentes, tal como se definen en la Directiva (UE) 2016/680, funciones que no se lleven a cabo necesariamente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluida la protección frente a las amenazas a la seguridad pública y su prevención, de tal forma que el tratamiento de datos personales para estos otros fines, en la medida en que esté incluido en el ámbito del Derecho de la Unión, entra en el ámbito de aplicación del presente Reglamento.

En lo que respecta al tratamiento de datos personales por parte de dichas autoridades competentes con fines que entren en el ámbito de aplicación del presente Reglamento, los Estados miembros deben tener la posibilidad de mantener o introducir disposiciones más específicas para adaptar la aplicación de las normas del presente Reglamento. Tales disposiciones pueden establecer de forma más precisa requisitos concretos para el tratamiento de datos personales con otros fines por parte de dichas autoridades competentes, tomando en consideración la estructura constitucional, organizativa y administrativa del Estado miembro en cuestión. Cuando el tratamiento de datos personales por organismos privados entre en el ámbito de aplicación del presente Reglamento, este debe disponer que los Estados miembros puedan, en condiciones específicas, limitar conforme a Derecho determinadas obligaciones y derechos siempre que dicha limitación sea una medida necesaria y proporcionada en una sociedad democrática para proteger intereses específicos importantes, entre ellos la seguridad pública y la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, inclusive la protección frente a las amenazas contra la seguridad pública y su prevención. Esto se aplica, por ejemplo, en el marco de la lucha contra el blanqueo de capitales o de las actividades de los laboratorios de policía científica.

Por consiguiente, los tratamientos de datos personales por parte de las autoridades competentes para los fines a los que se refiere el artículo 2.2.d) del RGPD quedan sujetos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Dicha Directiva se aprobó en la misma fecha que el RGPD y que la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, formando con ambas lo que se conoce como el paquete de reforma de protección de datos.

La Directiva 2016/680, cuya transposición a nuestro ordenamiento jurídico no se ha realizado todavía, estando en estos momentos en tramitación el correspondiente Anteproyecto de Ley, después de señalar en su artículo 1.1. que “La presente Directiva establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública”, delimita su ámbito subjetivo de aplicación en su artículo 2.1, de una manera claramente diferenciada a la contemplada en el RGPD:

> “1. La presente Directiva se aplica al tratamiento de datos personales por parte de las autoridades competentes a los fines establecidos en el artículo 1, apartado 1”.

Como ha señalado de manera reiterada esta Agencia, la Directiva 2016/680 viene a configurar un régimen especial, al que se someterían únicamente los tratamientos que la misma regula, frente al régimen general de protección de datos que se recoge en el Reglamento general de protección de datos. Por este motivo, las disposiciones del mismo serán de aplicación a todos los tratamientos llevados a cabo dentro del ámbito de aplicación del derecho de la Unión y que no estén regulados específicamente por la Directiva, tal y como se desprende del ámbito de aplicación establecido en el artículo 2 del Reglamento. Asimismo, el carácter de norma especial es igualmente predicable respecto de la norma que adapte el derecho español al Reglamento General de Protección de Datos (RGPD), constituida en el presente momento por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Y en este mismo sentido, hay que tener en cuenta que el régimen de la Directiva representa el mínimo exigible de garantía del derecho fundamental a la protección de datos en relación con los tratamientos sometidos a su ámbito de aplicación. De este modo las normas de derecho interno podrán recoger garantías adicionales del derecho, pero en ningún caso establecer un régimen más restrictivo del derecho fundamental que el recogido en la norma de derecho de la Unión. Así lo establece el artículo 1.3 de la Directiva al disponer que "La presente Directiva no impedirá a los Estados miembros ofrecer mayores garantías que las que en ella se establecen para la protección de los derechos y libertades del interesado con respecto al tratamiento de datos personales por parte de las autoridades competentes".

A este respecto, se debe partir de lo señalado en el artículo 3.7 de la Directiva que define como autoridad competente "toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública", o "cualquier otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública".

En este sentido, el considerando 11 de la Directiva señala que “Conviene por lo tanto que esos ámbitos estén regulados por una directiva que establezca las normas específicas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública. Entre dichas autoridades competentes no solo se deben incluir autoridades públicas tales como las autoridades judiciales, la policía u otras fuerzas y cuerpos de seguridad, sino también cualquier otro organismo o entidad en que el Derecho del Estado miembro haya confiado el ejercicio de la autoridad y las competencias públicas a los efectos de la presente Directiva. Cuando dicho organismo o entidad trate datos personales con fines distintos de los previstos en la presente Directiva, se aplica el Reglamento (UE) 2016/679. Así pues, el Reglamento (UE) 2016/679 se aplica en los casos en los que un organismo o entidad recopile datos personales con otros fines y proceda a su tratamiento para el cumplimiento de una obligación jurídica a la que esté sujeto. Por ejemplo, con fines de investigación, detección o enjuiciamiento de infracciones penales, las instituciones financieras conservan determinados datos personales que ellas mismas tratan y únicamente facilitan dichos datos personales a las autoridades nacionales competentes en casos concretos y de conformidad con el Derecho del Estado miembro. Todo organismo o entidad que trate datos personales en nombre de las citadas autoridades dentro del ámbito de aplicación de la presente Directiva debe quedar obligado por un contrato u otro acto jurídico y por las disposiciones aplicables a los encargados del tratamiento con arreglo a la presente Directiva, mientras que la aplicación del Reglamento (UE) 2016/679 permanece inalterada para el tratamiento de datos personales por encargados del tratamiento fuera del ámbito de aplicación de la presente Directiva”.

En este mismo sentido, el considerando 34 de la Directiva añade “El tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a amenazas para la seguridad pública, debe abarcar toda operación o conjunto de operaciones con datos personales o conjuntos de datos personales que se lleve a cabo con tales fines, ya sea de modo automatizado o no, y entre las que se incluye la recopilación, registro, organización, estructuración, almacenamiento, adaptación o modificación, recuperación, consulta, utilización, cotejo o combinación, limitación del tratamiento, supresión o destrucción de datos. En particular, las normas de la presente Directiva deben aplicarse a la transmisión de datos personales a los efectos de la presente Directiva a un destinatario que no esté sometido a la misma. Por «destinatario» debe entenderse toda persona física o jurídica, autoridad pública, servicio u otro organismo al que la autoridad competente comunique los datos personales de forma lícita. Si los datos personales fueron recopilados inicialmente por una autoridad competente para alguno de los fines previstos en la presente Directiva, el tratamiento de dichos datos para fines distintos de los previstos en la presente Directiva se regirá por lo dispuesto en el Reglamento (UE) 2016/679, siempre que dicho tratamiento esté autorizado por el Derecho de la Unión o del Estado miembro. En particular, las normas del Reglamento (UE) 2016/679 deben aplicarse a la transmisión de datos personales con fines no previstos en el ámbito de aplicación de la presente Directiva. Para el tratamiento de datos personales por parte de un destinatario que no sea una autoridad competente o que esté actuando como tal en el sentido de la presente Directiva y a quien una autoridad competente haya comunicado datos personales lícitamente, se estará a lo dispuesto en el Reglamento (UE) 2016/679. Al aplicar la presente Directiva, los Estados miembros deben poder precisar también la aplicación de las normas del Reglamento (UE) 2016/679, con sujeción a las condiciones establecidas en el mismo”.

El ejemplo mencionado en el considerando 11 es expresivo al indicar claramente que el tratamiento llevado a cabo por el sujeto obligado a comunicar los datos a una autoridad competente está sometido a las disposiciones del Reglamento general de protección de datos y no a las de la Directiva, sin perjuicio de que una vez comunicados los datos a la autoridad competente sí será aplicable a ese tratamiento lo establecido en la Directiva, pero sin que esa aplicación implique que el sujeto obligado se encuentra sujeto a las previsiones de ésta última, toda vez que la comunicación se habrá llevado a cabo al amparo del artículo 6.1 c) del reglamento.

Por consiguiente, los tratamientos de datos personales que lleven a cabo las empresas de seguridad, despachos de detectives privados y personal de seguridad privada, incluida la comunicación de datos a las Fuerzas y Cuerpos de Seguridad en cumplimiento de la obligación legal establecida en el artículo 14.2 de la Ley de Seguridad Privada, no están incluidos en el ámbito de aplicación de la Directiva 2016/680, quedando sujetos a lo dispuesto en el RGPD.

Este criterio lo viene a corroborar la propia LOPDGDD, que al regular en el artículo 22 los tratamientos con fines de videovigilancia, señala en su apartado 6 que "El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica".

Por el contrario, los tratamientos que realicen las empresas y personal de seguridad quedan sujetos a lo dispuesto en el citado precepto, "sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo".

II

La segunda cuestión que plantea la consulta se refiere a la incorporación de funcionalidades de reconocimiento facial en los sistemas de videovigilancia empleados en seguridad privada al amparo del artículo 42 de la Ley de Seguridad Privada, que a juicio de la consultante estaría permitido por el artículo 9.2.h) del RGPD, siendo suficiente a estos efectos que el usuario del servicio de seguridad sea titular del espacio a protegerse por la empresa de seguridad y que se trate de un dispositivo homologado por el Ministerio del Interior, conclusión de la que se difiere radicalmente.

Esta Agencia ha tenido ocasión de pronunciarse, recientemente, respecto de los sistemas de reconocimiento facial en su Informe 36/2020, relativo al uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online, en el que, como punto de partida, se señalaba que "**la existencia de un interés público no legitima cualquier tipo de tratamiento de datos personales, sino que deberá estarse, en primer lugar, a las condiciones que haya podido establecer el legislador, tal como prevé el propio artículo 6 del RGPD, en sus apartados 2 y 3, así como a los ya citados principios del artículo 5 del RGPD, especialmente a los de limitación de la finalidad y minimización de datos.**

Y en el caso de que vayan a ser objeto de tratamiento alguno o algunos de los datos personales incluidos en las categorías especiales de datos a los que se refiere el artículo 9.1. del RGPD, que concurra alguna de las circunstancias contempladas en su apartado 2 que levante la prohibición de tratamiento de dichos datos, establecida con carácter general en su apartado 1".

Por consiguiente, el empleo de tecnologías de reconocimiento facial en los sistemas de videovigilancia implica el tratamiento de datos biométricos, tal y como los define el artículo 4.14 del RGPD "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" y supone el tratamiento de categorías especiales de datos reguladas en el artículo 9 del RGPD, al tratarse de "datos biométricos dirigidos a identificar de manera unívoca a una persona física".

A este respecto, en el Informe 36/2020 de esta Agencia, anteriormente citado, se razonaba lo siguiente:

"No obstante, hay que adelantar que el RGPD no parece considerar a todo tratamiento de datos biométricos como tratamiento de categorías especiales de datos, ya que el artículo 9.1. se refiere a los "datos biométricos dirigidos a identificar de manera unívoca a una persona física", por lo que, de una interpretación conjunta de ambos preceptos parece dar a entender que los datos biométricos solo constituirían una categoría especial de datos en el caso de que se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física. En este sentido, parece que igualmente se pronuncia el Considerando 51 al señalar que "El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física".

Con igual criterio, el Protocolo de enmienda al Convenio para la Protección de Individuos con respecto al procesamiento de datos personales, aprobada por el Comité de Ministros en su 128º período de sesiones en Elsinore el 18 de mayo de 2018 (Convenio 108+) incluye únicamente como categorías especiales de datos, en su artículo 6.1 a los datos biométricos dirigidos a la identificación unívoca de una persona ("biometric data uniquely identifying a person"), sin incluir la referencia a la autenticación.

Al objeto de aclarar las dudas interpretativas que surgen respecto a la consideración de los datos biométricos como categorías especiales de datos puede acudirse a la distinción entre identificación biométrica y verificación/autenticación biométrica que establecía el Grupo del Artículo 29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas:

Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).

Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno).

Esta misma diferenciación se recoge en el Libro blanco sobre la inteligencia artificial de la Comisión Europea:

> “En lo que se refiere al reconocimiento facial, por «identificación» se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La «autenticación» (o «verificación»), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la misma. Este procedimiento se emplea, por ejemplo, en las puertas de control automatizado de fronteras empleadas en los controles fronterizos de los aeropuertos”.
>
> Atendiendo a la citada distinción, puede interpretarse que, de acuerdo con el artículo 4 del RGPD, el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación/autenticación. Sin embargo, y con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno).
>
> No obstante, esta Agencia considera que se trata de una cuestión compleja, sometida a interpretación, respecto de la cual no se pueden extraer conclusiones generales, debiendo atenderse al caso concreto según los datos tratados, las técnicas empleadas para su tratamiento y la consiguiente injerencia en el derecho a la protección de datos, debiendo, en tanto en cuanto no se pronuncia al respecto el Comité Europeo de Protección de Datos o los órganos jurisdiccionales, adoptarse, en caso de duda, la interpretación más favorable para la protección de los derechos de los afectados.”

En el presente caso, es indudable que la utilización de reconocimiento facial en los sistemas de videovigilancia empleados en el ámbito de la seguridad privada implicaría el tratamiento de un dato biométrico dirigido a identificar de una manera unívoca a una persona física, en un proceso de búsqueda de correspondencias uno-a-varios, constituyendo el tratamiento una categoría especial de datos cuyo tratamiento, en principio, se encuentra prohibido por el artículo 9.1. del RGPD.

En este sentido, el Comité Europeo de Protección de Datos, en sus “Guidelines 3/2019 on processing of personal data through video devices" considera el empleo de videovigilancia con reconocimiento facial como categoría especial de datos del artículo 9 del RGPD:

76. The use of video surveillance including biometric recognition functionality installed by private entities for their own purposes (e.g. marketing, statistical, or even security) will, in most cases, require explicit consent of all data subjects (Article 9 (2) (a)), however another suitable exception in Article 9 could also be applicable.

Example: To improve its service a private company replaces passenger identification check points within an airport (luggage drop-off, boarding) with video surveillance systems that use facial recognition techniques to verify the identity of the passengers that have chosen to consent to such a procedure. Since the processing falls under Article 9, the passengers, who will have previously given their explicit and informed consent, will have to enlist themselves at for example an automatic terminal in order to create and register their facial template associated with their boarding pass and identity.

III

Por consiguiente, para que sea lícito el tratamiento de los datos biométricos por los sistemas de reconocimiento facial integrado en un sistema de videovigilancia, debe concurrir alguna de las excepciones que levanten la prohibición de su tratamiento, conforme al apartado 2 del artículo 9 del RGPD.

A este respecto, el consultante considera que la exclusión o prohibición del artículo 9 del RGPD, en relación al tratamiento de categorías especiales de datos personales, no resultaría de aplicación al ámbito sectorial de la Seguridad Privada, rigiendo la excepción del apartado 2 de este artículo, excepción que estaría prevista para el tratamiento de datos para las empresas y personal de seguridad privada en la normativa de seguridad privada dentro del derecho interno de España.

Sin embargo, dicha afirmación no puede compartirse por esta Agencia al no existir el imprescindible amparo legal, en los términos exigidos por el artículo 9.2.g) del RGPD y por la doctrina constitucional.

En este sentido, procede traer a colación lo ya indicado por esta Agencia en la ya citado Informe 36/2020, en relación con un supuesto de tratamiento de datos personales basado en la existencia, al igual que en el presente caso, de un interés público:

V

La siguiente cuestión que se plantea en la consulta es si el tratamiento de los datos biométricos por los sistemas de reconocimiento facial en los procesos de evaluación online podría ampararse en la existencia de un interés público esencial conforme al artículo 9.2.g) del RGPD:

> 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.

Tal y como señalábamos anteriormente, el tratamiento de datos personales necesarios para la prestación del servicio público de educación superior se legitima, con carácter general, en la existencia de un interés público al amparo de lo previsto en el artículo 6.1.e) del RGPD. Sin embargo, tratándose de categorías especiales de datos, el supuesto contemplado en la letra g) del artículo 9.2. no se refiere solo a la existencia de un interés público, tal y como hace en muchos otros de sus preceptos el RGPD, sino que es el único precepto del RGPD que requiere que el mismo sea “esencial”, adjetivo que viene a cualificar dicho interés público, habida cuenta de la importancia y necesidad de mayor protección de los datos tratados.

Dicho precepto encuentra su precedente en el artículo 8.4 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos: “4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control”. No obstante, de su lectura resulta un mayor rigor en a nueva regulación por el RGPD, ya que se sustituye el adjetivo “importantes” por “esencial” y no se permite que la excepción pueda establecerse por las autoridades de control.

En relación con lo que debe entenderse por interés público esencial, debe tenerse igualmente en cuenta la Jurisprudencia del Tribunal Europeo de Derechos Humanos, que al amparo del artículo 8 del Convenio Europeo de Derechos Humanos, viene considerando que el tratamiento de datos personales constituye una injerencia lícita en el derecho del respeto de la vida privada y sólo puede llevarse a cabo si se realiza de conformidad con la ley, sirve a un fin legítimo, respeta la esencia de los derechos y libertades fundamentales y es necesario y proporcionado en una sociedad democrática para alcanzar un fin legítimo (D.L. contra Bulgaria, nº 7472/14, 19 de mayo de 2016, Dragojević contra Croacia, nº 68955/11, 15 de enero de 2015, Peck contra Reino Unido, nº 44647/98, 28 de enero de 2003, Leander contra Suecia, n.o 9248/81, 26 de marzo de 1987, entre otras). Como señala en la última sentencia citada, «el concepto de necesidad implica que la

injerencia responda a una necesidad social acuciante y, en particular, que sea proporcionada con el fin legítimo que persigue».

Asimismo, debe tenerse en cuenta la doctrina del Tribunal Constitucional respecto a las restricciones al derecho fundamental a la protección de datos, que sintetiza en su sentencia 292/2000, de 30 de noviembre, en la que después de configurar el derecho fundamental a la protección de datos personales como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso, analiza los límites del mismo, señalando en lo siguiente:

> Más concretamente, en las Sentencias mencionadas relativas a la protección de datos, este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, F. 7; 196/1987, de 11 de diciembre [RTC 1987, 196] , F. 6; y respecto del art. 18, la STC 110/1984, F. 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental. Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero [RTC 1994, 57] , F. 6; 18/1999, de 22 de febrero [RTC 1999, 18] , F. 2).

Justamente, si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional, el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos. Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen. Como lo conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga. Y así será cuando la Ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro Poder Público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese Poder Público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, almacenamiento, tratamiento, uso y cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional […]". (Fundamento Jurídico 11)

"De un lado, porque si bien este Tribunal ha declarado que la Constitución no impide al Estado proteger derechos o bienes jurídicos a costa del sacrificio de otros igualmente reconocidos y, por tanto, que el legislador pueda imponer limitaciones al contenido de los derechos fundamentales o a su ejercicio, también hemos precisado que, en tales supuestos, esas limitaciones han de estar justificadas en la protección de otros derechos o bienes constitucionales (SSTC 104/2000, de 13 de abril [RTC 2000, 104] , F. 8 y las allí citadas) y, además, han de ser proporcionadas al fin perseguido con ellas (SSTC 11/1981, F. 5, y 196/1987, F. 6). Pues en otro caso incurrirían en la arbitrariedad proscrita por el art. 9.3 CE.

De otro lado, aun teniendo un fundamento constitucional y resultando proporcionadas las limitaciones del derecho

fundamental establecidas por una Ley (STC 178/1985 [RTC 1985, 178]), éstas pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación. Conclusión que se corrobora en la jurisprudencia del Tribunal Europeo de Derechos Humanos que ha sido citada en el F. 8 y que aquí ha de darse por reproducida. Y ha de señalarse, asimismo, que no sólo lesionaría el principio de seguridad jurídica (art. 9.3 CE), concebida como certeza sobre el ordenamiento aplicable y expectativa razonablemente fundada de la persona sobre cuál ha de ser la actuación del poder aplicando el Derecho (STC 104/2000, F. 7, por todas), sino que al mismo tiempo dicha Ley estaría lesionando el contenido esencial del derecho fundamental así restringido, dado que la forma en que se han fijado sus límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio (SSTC 11/1981, F. 15; 142/1993, de 22 de abril [RTC 1993, 142] , F. 4, y 341/1993, de 18 de noviembre [RTC 1993, 341] , F. 7). De suerte que la falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho fundamental es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción. Y al producirse este resultado, más allá de toda interpretación razonable, la Ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien ha de aplicarla, menoscabando así tanto la eficacia del derecho fundamental como la seguridad jurídica […]”. (FJ 15).

“Más concretamente, en relación con el derecho fundamental a la intimidad hemos puesto de relieve no sólo la necesidad de que sus posibles limitaciones estén fundadas en una previsión legal que tenga justificación constitucional y que sean proporcionadas (SSTC 110/1984, F. 3, y 254/1993, F. 7) sino que la Ley que restrinja este derecho debe expresar con precisión todos y cada uno de los presupuestos materiales de la medida limitadora. De no ser así, mal cabe entender que la resolución judicial o el acto administrativo que la aplique estén fundados en la Ley, ya que lo que ésta ha hecho, haciendo dejación de sus funciones, es apoderar a otros Poderes Públicos para que sean ellos quienes fijen los límites al derecho fundamental (SSTC 37/1989, de 15 de febrero [RTC 1989, 37], y 49/1999, de 5 de abril [RTC 1999, 49]).

De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando

> concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación. […] (FJ 16)".

Asimismo, nuestro Tribunal Constitucional ha tenido ya la ocasión de pronunciarse específicamente sobre el artículo 9.2.g) del RGPD, como consecuencia de la impugnación del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, introducido por la disposición final tercera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, relativo a la legitimación de la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales, precepto que fue declarado inconstitucional por la Sentencia num. 76/2019 de 22 mayo.

Dicha sentencia analiza, en primer término, el régimen jurídico al que se encuentra sometido el tratamiento de las categorías especiales de datos en el RGPD:

> De acuerdo con el apartado 1 del art. 9 RGPD, está prohibido el tratamiento de datos personales que revelen las opiniones políticas, del mismo modo que lo está el tratamiento de datos personales que revelen el origen étnico o racial, 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 la orientación sexual de una persona física. No obstante, el apartado 2 del mismo precepto autoriza el tratamiento de todos esos datos cuando concurra alguna de las diez circunstancias allí previstas [letras a) a j)]. Algunas de esas circunstancias tienen un ámbito de aplicación acotado (laboral, social, asociativo, sanitario, judicial, etc.) o responden a una finalidad determinada, por lo que, en sí mismas, delimitan los tratamientos específicos que autorizan como excepción a la regla general. Además, la eficacia habilitante de varios de los supuestos allí previstos está condicionada a que el Derecho de la Unión o el de los Estados miembros los prevean y

> regulen expresamente en su ámbito de competencias: es el caso de las circunstancias recogidas en las letras a), b), g), h), i) y j).
> El tratamiento de las categorías especiales de datos personales es uno de los ámbitos en los que de manera expresa el Reglamento General de Protección de Datos ha reconocido a los Estados miembros "margen de maniobra" a la hora de "especificar sus normas", tal como lo califica su considerando 10. **Este margen de configuración legislativa se extiende tanto a la determinación de las causas habilitantes para el tratamiento de datos personales especialmente protegidos -es decir, a la identificación de los fines de interés público esencial y la apreciación de la proporcionalidad del tratamiento al fin perseguido, respetando en lo esencial el derecho a la protección de datos- como al establecimiento de "medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" [art. 9.2 g) RGPD]. El Reglamento contiene, por tanto, una obligación concreta de los Estados miembros de establecer tales garantías, en el caso de que habiliten para tratar los datos personales especialmente protegidos.**

En relación con el primero de los requisitos exigidos por el artículo 9.2.g), la invocación de un interés público esencial y la necesaria especificación del mismo, el Alto Tribunal recuerda lo señalado en su sentencia 292/2000 en la que se rechazaba que la identificación de los fines legítimos de la restricción pudiera realizarse mediante conceptos genéricos o fórmulas vagas, considerando que la restricción del derecho fundamental a la protección de datos personales no puede estar basada, por sí sola, en la invocación genérica de un indeterminado "interés público" :

> En la ya citada STC 292/2000 (RTC 2000, 292) , en la que también se enjuició una injerencia legislativa en el derecho a la protección de datos personales, rechazamos que la identificación de los fines legítimos de la restricción pudiera realizarse mediante conceptos genéricos o fórmulas vagas:
> "16. [...] De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que

hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación.

17. En el caso presente, el empleo por la LOPD (RCL 2018, 1629) en su art. 24.1 de la expresión "funciones de control y verificación", abre un espacio de incertidumbre tan amplio que provoca una doble y perversa consecuencia. De un lado, al habilitar la LOPD a la Administración para que restrinja derechos fundamentales invocando semejante expresión está renunciando a fijar ella misma los límites, apoderando a la Administración para hacerlo. Y de un modo tal que, como señala el Defensor del Pueblo, permite reconducir a las mismas prácticamente toda actividad administrativa, ya que toda actividad administrativa que implique entablar una relación jurídica con un administrado, que así será prácticamente en todos los casos en los que la Administración necesite de datos personales de alguien, conllevará de ordinario la potestad de la Administración de verificar y controlar que ese administrado ha actuado conforme al régimen jurídico administrativo de la relación jurídica entablada con la Administración. Lo que, a la vista del motivo de restricción del derecho a ser informado del art. 5 LOPD, deja en la más absoluta incertidumbre al ciudadano sobre en qué casos concurrirá esa circunstancia (si no en todos) y sume en la ineficacia cualquier mecanismo de tutela jurisdiccional que deba enjuiciar semejante supuesto de restricción de derechos fundamentales sin otro criterio complementario que venga en ayuda de su control de la actuación administrativa en esta materia.

Iguales reproches merece, asimismo, el empleo en el art. 24.2 LOPD de la expresión "interés público" como fundamento de la imposición de límites a los derechos fundamentales del art. 18.1 y 4 CE, pues encierra un grado de incertidumbre aún mayor. Basta reparar en que toda actividad administrativa, en último término, persigue la salvaguardia de intereses generales, cuya consecución constituye la finalidad a la que debe servir con objetividad la Administración con arreglo al art. 103.1 CE."

Esta argumentación es plenamente trasladable al presente enjuiciamiento. De igual modo, por tanto, debemos concluir que la legitimidad constitucional de la restricción del derecho fundamental a la protección de datos personales no puede estar basada, por sí sola, en la invocación genérica de un indeterminado "interés público". Pues en otro caso el legislador habría trasladado a los partidos políticos -a quienes la disposición impugnada habilita para recopilar datos personales relativos a las

> opiniones políticas de las personas en el marco de sus actividades electorales- el desempeño de una función que solo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente sus límites y su regulación.
> Tampoco puede aceptarse, por igualmente imprecisa, la finalidad aducida por el abogado del Estado, que se refiere al funcionamiento del sistema democrático, pues también encierra un grado elevado de incertidumbre y puede suponer un razonamiento circular. Por un lado, los partidos políticos son de por sí "cauces necesarios para el funcionamiento del sistema democrático" (por todas, STC 48/2003, de 12 de marzo (RTC 2003, 48) , FJ 5); y, por otro lado, todo el funcionamiento del sistema democrático persigue, en último término, la salvaguardia de los fines, valores y bienes constitucionales, pero ello no alcanza a identificar la razón por la cual haya de restringirse el derecho fundamental afectado.
> Finalmente, debe precisarse que no es necesario que se pueda sospechar, con mayor o menor fundamento, que la restricción persiga una finalidad inconstitucional, o que los datos que se recopilen y procesen resultarán lesivos para la esfera privada y el ejercicio de los derechos de los particulares. Es suficiente con constatar que, al no poderse identificar con la suficiente precisión la finalidad del tratamiento de datos, tampoco puede enjuiciarse el carácter constitucionalmente legítimo de esa finalidad, ni, en su caso, la proporcionalidad de la medida prevista de acuerdo con los principios de idoneidad, necesidad y proporcionalidad en sentido estricto.

Por otro lado, en cuanto a las garantías que debe adoptar el legislador, la citada sentencia núm. 76/2019 de 22 mayo, después de recordar que “A la vista de los potenciales efectos intrusivos en el derecho fundamental afectado que resultan del tratamiento de datos personales, la jurisprudencia de este Tribunal le exige al legislador que, además de cumplir los requisitos anteriormente mencionados, también establezca garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental”, analiza cuál es la norma que debe contener las citadas garantías:

> “Por tanto, la resolución de la presente impugnación exige que aclaremos una duda suscitada con respecto al alcance de nuestra doctrina sobre las garantías adecuadas, que consiste en determinar si las garantías adecuadas frente al uso de la informática deben contenerse en la propia ley que autoriza y

regula ese uso o pueden encontrarse también en otras fuentes normativas.

La cuestión solo puede tener una respuesta constitucional. La previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. Solo ese entendimiento es compatible con la doble exigencia que dimana del art. 53.1 CE (RCL 1978, 2836) para el legislador de los derechos fundamentales: la reserva de ley para la regulación del ejercicio de los derechos fundamentales reconocidos en el capítulo segundo del título primero de la Constitución y el respeto del contenido esencial de dichos derechos fundamentales.

Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas -unas veces- de predeterminación normativa y -otras- de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales. Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares" (FJ 8).

Por consiguiente, el tratamiento de datos biométricos al amparo del artículo 9.2.g) requiere que esté previsto en una norma de derecho europeo o nacional, debiendo tener en este último caso dicha norma, según la doctrina constitucional citada y lo previsto en el artículo 9.2 de la LOPDGDD, rango de ley. Dicha ley deberá, además especificar el interés público esencial que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse, estableciendo las reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, sin que sea suficiente, a estos efectos, la invocación genérica de un interés público. Y dicha ley deberá establecer, además, las garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos.

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

> "En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la 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; SSTC 66/1995, de 8 de mayo [RTC 1995, 66] , F. 5; 55/1996, de 28 de marzo [RTC 1996, 55] , FF. 7, 8 y 9; 270/1996, de 16 de diciembre [RTC 1996, 270] , F. 4.e; 37/1998, de 17 de febrero [RTC 1998, 37] , F. 8; 186/2000, de 10 de julio [RTC 2000, 186] , F. 6)."

En el presente caso, ya hemos citado cómo el artículo 22 de la LPDGDD regula los tratamiento con fines de videovigilancia cuya legitimación se encuentra, tal y como señaló en su Dictamen el Consejo de Estado y ha recogido la Ley en su Exposición de Motivos, en la existencia de una finalidad de interés público incardinable en el artículo 6.1.e) del Reglamento general, al tener por finalidad "preservar la seguridad de las personas y bienes, así como de sus instalaciones", un objetivo que sobrepasa los meros intereses legítimos de un particular.

El citado precepto regula el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones, estableciendo una serie de requisitos y garantías:

> Artículo 22. Tratamientos con fines de videovigilancia.
>
> 1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.
>
> 2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.

7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica.

En el ámbito de la seguridad privada, dicha regulación debe completarse con lo dispuesto en su normativa específica, regulando la Ley de Seguridad Privada, en su artículo 42, los servicios de videovigilancia:

Artículo 42. Servicios de videovigilancia.

1. Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas.

Cuando la finalidad de estos servicios sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales.

No tendrán la consideración de servicio de videovigilancia la utilización de cámaras o videocámaras cuyo objeto principal sea la comprobación del estado de instalaciones o bienes, el control de accesos a aparcamientos y garajes, o las actividades que se desarrollan desde los centros de control y otros puntos, zonas o áreas de las autopistas de peaje. Estas funciones podrán realizarse por personal distinto del de seguridad privada.

2. No se podrán utilizar cámaras o videocámaras con fines de seguridad privada para tomar imágenes y sonidos de vías y espacios públicos o de acceso público salvo en los supuestos y en los términos y condiciones previstos en su normativa específica, previa autorización administrativa por el órgano competente en cada caso. Su utilización en el interior de los domicilios requerirá el consentimiento del titular.

3. Las cámaras de videovigilancia que formen parte de medidas de seguridad obligatorias o de sistemas de recepción, verificación y, en su caso, respuesta y transmisión de alarmas, no requerirán autorización administrativa para su instalación, empleo o utilización.

4. Las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad. Cuando las mismas se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, se aportarán, de propia iniciativa o a su requerimiento, a las Fuerzas y Cuerpos de Seguridad competentes, respetando los criterios de conservación y custodia de las mismas para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales.

5. La monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de videovigilancia estará sometida a lo previsto en la normativa en materia de protección de datos de carácter personal, y especialmente a los principios de proporcionalidad, idoneidad e intervención mínima.

6. En lo no previsto en la presente ley y en sus normas de desarrollo, se aplicará lo dispuesto en la normativa sobre videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad.

Como puede observarse, **los tratamientos de videovigilancia regulados en la LOPDGDD y en la LSP, se refieren exclusivamente a los tratamientos dirigidos a captar y grabar imágenes y sonidos, pero no incluyen los tratamientos de reconocimiento facial**, que es un tratamiento radicalmente distinto al incorporar un dato biométrico, como recuerda el propio RGPD en su Considerando 51 al señalar que “El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física”.

Por consiguiente, la incorporación a los sistemas de videovigilancia, dirigidos a la captación y grabación de imágenes y sonidos, de aplicaciones de reconocimiento facial va a implicar el tratamiento de datos biométricos, respecto de los cuales las autoridades de protección de datos venían advirtiendo de los riesgos que implican para los derechos de las personas.

En este sentido, el Grupo del 29, en su **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.”

Previamente, en el **Documento de trabajo sobre biometría, adoptado el 1 de agosto de 2003**, el Grupo del 29 destacaba que “**Una utilización amplia y sin control de la biometría es preocupante desde el punto de vista de la protección de los derechos y libertades fundamentales de las personas**. Este tipo de datos es de una naturaleza especial, ya que tienen que ver con las características comportamentales y fisiológicas de una persona y pueden permitir su identificación inequívoca”. Asimismo, en dicho documento se destacaban alguno de los riesgos que implicaban el uso de dichas tecnologías en casos como el que nos ocupa, en los que “la identificación sólo puede realizarse almacenando los datos de referencia en una base de datos centralizada, porque, con objeto de averiguar la identidad del interesado, el sistema debe comparar sus plantillas o datos brutos (imagen) con las plantillas o datos brutos de todas las personas cuyos datos ya están almacenados de forma centralizada”.

Asimismo, cita otros riesgos sustanciales, como el hecho de que el tratamiento pueda realizarse sin conocimiento del interesado, la posible generalización de su uso y los errores que pueden producirse:

> “Todo esto ocurre también con otros sistemas biométricos, como los basados en el análisis de la pulsación sobre las teclas o el reconocimiento facial a distancia, gracias a las características de la tecnología utilizada. **El aspecto problemático es, por una parte, que esta recogida y este tratamiento de datos puede hacerse sin el conocimiento del interesado y, por la otra, que independientemente de su fiabilidad actual, esas tecnologías biométricas se prestan a una utilización generalizada a causa de su "bajo nivel de intrusión".** Por consiguiente, parece necesario establecer garantías específicas a este respecto
>
> […]

Los errores que se producen dentro de los sistemas biométricos pueden tener graves consecuencias para la persona y, en particular, la denegación errónea a personas autorizadas y la aceptación errónea de personas no autorizadas pueden provocar serios problemas a muy diferentes niveles".

Posteriormente, en el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, adoptado el 27 de abril de 2012, el Grupo del 29, después de señalar que "Las tecnologías biométricas están estrechamente vinculadas a determinadas características de una persona y algunas de ellas pueden utilizarse para revelar datos sensibles. Además, muchas permiten el seguimiento, rastreo o elaboración del perfil de las personas y, como tal, su potencial impacto en la intimidad y el derecho a la protección de los datos de las personas es elevado", identifica los principales riesgos para la privacidad derivados del empleo del reconocimiento facial:

Los riesgos para la protección de datos asociados al uso de los sistemas de reconocimiento facial pueden describirse de la manera siguiente:

• Precisión: si la calidad de las imágenes no puede garantizarse, existe el riesgo de que la exactitud se vea comprometida. Si no se capta una cara (oscurecida por el pelo o por un sombrero) está claro que la correspondencia o categorización no podrá darse sin un alto índice de error. Las variaciones en la pose y la iluminación siguen siendo un enorme reto para el reconocimiento facial, que afecta en gran medida a la precisión.

• Impacto: el impacto específico en la protección de datos de un determinado sistema de reconocimiento facial dependerá de su finalidad y circunstancias particulares. Un sistema de categorización para el recuento de visitantes a una atracción, sin capacidad de registro, tendrá un impacto diferente en la protección de datos que el de un sistema utilizado para la vigilancia discreta por las autoridades con funciones coercitivas a fin de identificar a posibles alborotadores.

• Consentimiento y transparencia: un riesgo de protección de datos que no está presente en muchos otros tipos de tratamiento de datos biométricos es el hecho de que las imágenes pueden capturarse y tratarse desde una serie de puntos de vista, condiciones ambientales y sin el conocimiento del interesado. En el Dictamen 15/2011 sobre la definición del consentimiento, el Grupo de Trabajo destaca el hecho de que para que el consentimiento constituya una base jurídica para el tratamiento, debe ser «informado». Si el interesado no tiene conocimiento del tratamiento de imágenes a efectos del reconocimiento facial, no puede dar un consentimiento informado. Incluso si el interesado es consciente de que hay una cámara funcionando, puede no distinguirse si se trata de un sistema de TVCC que funcione en directo o

que grabe las imágenes, o de una lente que capture imágenes para un sistema de reconocimiento facial.

• Fin o fines ulteriores del tratamiento: una vez capturadas, de forma legítima o ilegítima, las imágenes digitales pueden fácilmente compartirse o copiarse para su tratamiento en sistemas diferentes de aquellos para los que estaban destinadas originalmente. Esto resulta evidente en el ámbito de los medios de comunicación social, donde los usuarios cargan sus fotografías personales para compartirlas con su familia, amigos y compañeros. Una vez en la plataforma de medios sociales, las imágenes están disponibles para su reutilización por la propia plataforma para una amplia gama de fines, algunos de los cuales pueden introducirse en la plataforma incluso después de que la imagen haya sido tomada o cargada.

• Vinculación: un gran número de servicios en línea permiten a los usuarios cargar una imagen para vincularla con el perfil del usuario. El reconocimiento facial puede utilizarse para vincular los perfiles de diferentes servicios en línea (a través de la imagen del perfil), pero también entre el mundo en línea y fuera de línea. No está fuera de lo posible tomar una fotografía de una persona en la calle y determinar su identidad en tiempo real buscando en estas imágenes de perfil público. Servicios de terceros también pueden rastrear fotografías de perfil y otras fotografías públicamente disponibles para crear grandes colecciones de imágenes a fin de asociar una identidad del mundo real con tales imágenes.

• Seguimiento/elaboración de perfiles: también podría utilizarse un sistema de identificación si no se conoce la identidad real de una persona. Podría utilizarse un sistema de reconocimiento facial en un centro comercial o espacio público similar para seguir las rutas y costumbres de los consumidores individuales. La finalidad podría ser una gestión eficaz de las colas o la colocación de productos con el fin de mejorar la experiencia del cliente. No obstante, junto con la capacidad para seguir o localizar a un individuo concreto está la capacidad para elaborar perfiles y enviar publicidad u otros servicios específicos.

• Tratamiento de datos sensibles: como ya se ha mencionado, el tratamiento de datos biométricos podría utilizarse para determinar datos sensibles, en especial aquellos con señales visuales tales como la raza, grupo étnico o quizá una enfermedad.

• Revocabilidad: un individuo puede cambiar fácilmente su apariencia (barba, gafas, sombrero, etc.) y burlar fácilmente los sistemas de reconocimiento facial, especialmente cuando operan en un entorno no controlado. No obstante, las principales características faciales de una persona son estables en el tiempo y los sistemas también pueden mejorar el reconocimiento recogiendo y asociando diferentes «caras» conocidas de una persona.

• Protección anti-suplantación: muchos sistemas de reconocimiento facial son fáciles de suplantar, pero los fabricantes intentan mejorar esta deficiencia con técnicas tales como la imagen en

3D o la grabación en vídeo. Sin embargo, la mayoría de los sistemas básicos utilizados en aplicaciones públicas no incluyen este tipo de protección.

Más recientemente, el Comité Europeo de Protección de Datos (European Data Protection Board, EDPB), en sus Guidelines 3/2019 on processing of personal data through video devices, adoptadas el 29 de enero de 2020, reincide en los mayores riesgos que para los derechos de los afectados implica el empleo de tegnologías de reconocimiento facial, y la necesidad de que las mismas respeten los principios del RGPD:

> 73. The use of biometric data and in particular facial recognition entail heightened risks for data subjects' rights. It is crucial that recourse to such technologies takes place with due respect to the principles of lawfulness, necessity, proportionality and data minimisation as set forth in the GDPR. Whereas the use of these technologies can be perceived as particularly effective, controllers should first of all assess the impact on fundamental rights and freedoms and consider less intrusive means to achieve their legitimate purpose of the processing.

Por consiguiente, no puede admitirse, tal y como pretende la consulta, que la legitimación reconocida para los sistemas de videovigilancia, dirigida solo a la captación y grabación de la imagen y el sonido, abarque otras tecnologías mucho más intrusivas para la privacidad como pueda ser el reconocimiento facial u otras medidas biométricas como el reconocimiento de la forma de andar o el reconocimiento de voz.

Por el contrario, la regulación actual se considera insuficiente para permitir la utilización de técnicas de reconocimiento facial en sistemas de videovigilancia empleados por la seguridad privada, al no cumplir los requisitos anteriormente señalados, siendo necesario que se aprobara una norma con rango de ley que justificara específicamente en qué medida y en qué supuestos, la utilización de dichos sistemas respondería a un interés público esencial, definiendo dicha norma legal, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías técnicas, organizativas y procedimentales adecuadas, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos.

Dicha norma, en el caso de tramitarse, deberá ser preceptivamente informada por esta Agencia, momento en el cual podría valorarse si la misma

se ajusta a los criterios señalados, sin que, apriorísticamente, se puede establecer un criterio taxativo por nuestra parte. No obstante, si puede adelantarse que, atendiendo al principio de proporcionalidad y al juicio de necesidad, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia, la existencia de otras medidas que permiten la protección de las personas, bienes e instalaciones con una menor intrusión en el derecho de los afectados, exigiría una especial justificación de la necesidad de optar por el reconocimiento facial respecto de dichas otras medidas.

Así, esta Agencia considera que existen supuestos excepcionales en los que podría quedar justificado el empleo de sistemas de reconocimiento facial siempre que la legislación, en los términos anteriormente señalados, así lo prevea, como podría ser el caso de las infraestructuras críticas, entendiendo por tales, conforme a la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, aquéllas cuyo "funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales". En este caso, la adecuada protección de las mismas tiene por finalidad garantizar la seguridad de los ciudadanos y el correcto funcionamiento de los servicios esenciales, por lo que la autorización por el legislador del empleo de técnicas de reconocimiento facial, estableciendo las garantías adecuadas, podría considerarse proporcional.

Sin embargo, la autorización, con carácter general, del empleo de sistemas de reconocimiento facial en los sistemas de videovigilancia empleados por la seguridad privada, tal y como se plantea en la consulta, sería considerada, por esta Agencia, como desproporcionada, dada la intrusión y los riesgos que supone para los derechos fundamentales de los ciudadanos.