ASUNTO: Consulta Previa (Art. 36 RGPD)

- **Ref. REGAGE25e00024730156**

En virtud de las competencias atribuidas a la Agencia Española de Protección de Datos (AEPD) por el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y en virtud de los poderes que el artículo 58 del mismo otorga a este organismo, la Presidencia de la Agencia Española de Protección de Datos da respuesta escrita a la solicitud de consulta previa presentada, todo ello en cumplimiento de lo previsto en el artículo 36 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 o RGPD):

I. RESUMEN DE LA SOLICITUD DE CONSULTA PREVIA

Con fecha 27 de marzo de 2025 tuvo entrada en esta Agencia solicitud de consulta previa relativa al artículo 36 del RGPD, que afecta a un tratamiento de datos personales que tiene por finalidad el control de accesos a la (…) Guardia Civil, (…). Las operaciones de tratamiento que -según se informa- se incluyen en la solicitud de consulta, afectan tanto a visitantes al recinto como a trabajadores y a los residentes de las viviendas que se encuentran dentro del recinto. Adicionalmente, en la documentación aportada se pone de manifiesto que se trata de un sistema de autenticación sin creación de base de datos centralizada, basado en información biométrica, con generación biométrica en el tótem de recogida de datos, y la plantilla biométrica conservada por el usuario.

En la consulta planteada se manifiesta que la base legal del tratamiento y el levantamiento de la prohibición legalmente requerida por tratarse los datos biométricos de datos de categorías especiales pueda ser la prevista en la Ley 8/2011 de medidas para la protección de infraestructuras críticas y en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

En este caso, las instalaciones a las que se circunscribe el análisis es (…) la Guardia Civil, el cual se compone de varios edificios e instalaciones de distinta naturaleza, que incluye inmuebles que se consideran esenciales para las funciones a desempeñar, (…). Así las cosas, si bien no existen dudas de la necesidad de protección de una infraestructura de tal naturaleza, correspondía al propio consultante su distinción y justificación de necesidad en cada caso o espacio específico.

No hay que descartar que esta identificación de zonas pudiera llevar a que haya espacios que requieran una mayor protección y que justifiquen, más si cabe, el uso de tecnologías biométricas adecuadas. Del mismo modo, podría haber otros espacios con

necesidades de seguridad menores, donde el control de acceso pudiera realizarse a través de otros canales menos intrusivos con el derecho fundamental a la protección de datos personales. Ahora bien, sin perjuicio de la posibilidad de estas diferenciaciones, hay que abordar conjuntamente todo el espacio del que se trata, por cuanto como unidad contará homogéneamente con unos mínimos de seguridad necesarios. Esto es, una necesidad de seguridad que se aplica al conjunto como infraestructura esencial para la seguridad pública que sin duda merece una protección específica. Todo ello, sin perjuicio y como se ha señalado de que pueda haber espacios que requieran de una necesidad más intensa de protección y, por tanto, de medidas adecuadas y proporcionales.

Es evidente que no toda instalación pública justifica automáticamente el uso de tecnologías biométricas, sino que debe justificarse dicha necesidad en un informe de evaluación de impacto en la protección de datos (EIPD), que analice el riesgo y la proporcionalidad del tratamiento. Tal justificación se ha recogido, en el presente caso, (…).

II. ANÁLISIS DE LA PROPUESTA PLANTEADA

A. FINES

Como se indica en la documentación aportada y como obra en el inventario de actividades de tratamiento del Ministerio de Interior, el tratamiento denominado COSEIN-ACCESOS tiene por finalidad la de:

> *"Identificación y control de personas ajenas, residentes, vehículos que acceden o autorizados a estacionar en el interior. Gestión sistemas acceso con identificación mediante tarjetas, biometría, u otro tipo que suponga tratamiento de datos personales."*

En la consulta se afirma la finalidad de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales así como se sostiene una relación de hechos realizados contra este tipo de edificios de manera genérica.

Así las cosas y en principio, no se trataría de un nuevo tratamiento y la novedad radicaría, exclusivamente, en la implementación de un sistema de biometría para automatizar el acceso de las personas a las zonas y el tiempo definidos en la autorización previa.

B. BASE LEGAL Y CONTEXTO NORMATIVO

Procede abordar la base legal y para ello hay que tener en cuenta todo un conjunto normativo concurrente. En el propio Inventario de tratamientos COSEIN-ACCESOS, se señala que la base legal (legitimación) es el cumplimiento de una obligación legal; artículo 6.1.c del RGPD. Y el consentimiento del interesado; artículo 6.1.a del RGPD. Igualmente,

en la consulta planteada se manifiesta que la base legal del tratamiento y el levantamiento de la prohibición legalmente requerida por tratarse los datos biométricos de datos de categorías especiales pudiera ser la prevista en la Ley 8/2011 de medidas para la protección de infraestructuras críticas. También se afirma la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. En la misma línea, la base legal tendría su fundamento en el artículo 11.1.c de la Ley Orgánica 2/1986 de Fuerzas y Cuerpos de Seguridad, en la competencia que se asigna a las Fuerzas y Cuerpos de Seguridad para *"Vigilar y proteger los edificios e instalaciones públicos que lo requieran"*.

Pues bien, de una parte, cabe tener en cuenta la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. En razón de su objeto (artículo 1) y ámbito de aplicación (artículo 2.1) esta ley se aplicaría a tratamientos de datos personales en una instalación biométrica de seguridad instalada por cuanto el fin del tratamiento sea la prevención de delitos o amenazas contra la seguridad pública. Como luego se detalla, al tratarse de datos biométricos como categorías especiales de datos en el sentido del artículo 13 Ley Orgánica 7/2021, de 26 de mayo, según su apartado 1 a), que contempla expresamente que este tipo de tratamiento será lícito cuando "Se encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea." En este punto, la normativa aplicable que confiere la cobertura jurídica a este tratamiento es, esencialmente, la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. El artículo 11 de esta Ley Orgánica 2/1986 dispone en su apartado primero que "Las Fuerzas y Cuerpos de Seguridad del Estado tienen como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana mediante el desempeño de las siguientes funciones:" [y por lo que ahora más interesa…] c) Vigilar y proteger los edificios e instalaciones públicos que lo requieran." También, con carácter más genérico "f) Prevenir la comisión de actos delictivos."

Por cuanto a la consideración de las instalaciones a proteger como posibles infraestructuras críticas, cabe tener en cuenta la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo. Esta Directiva se encuentra actualmente en transposición al ordenamiento jurídico español a través de un borrador de anteproyecto de Ley. En tanto se materializa la transposición, resulta de aplicación la Ley 8/2011, de 28 de abril y dicha ley exceptúa de su aplicación a las infraestructuras dependientes de las Fuerzas y Cuerpos de Seguridad en el sentido siguiente:

> *2. Se exceptúan de su aplicación las infraestructuras dependientes del Ministerio de Defensa y de las Fuerzas y Cuerpos de Seguridad, que se regirán, a efectos de control administrativo, por su propia normativa y procedimientos.*

Así las cosas, la Ley 8/2011 no sería de aplicación.

En cualquier caso, la eventual presencia de elementos o funciones calificables como infraestructura crítica en los términos de la Ley 8/2011 constituye un indicio objetivo de una intensa necesidad de una adecuada protección física y lógica de las instalaciones. Ello coadyuva y refuerza la necesidad, en su caso, de las medidas biométricas proporcionales de seguridad.

Asimismo y de otra parte, el anteproyecto de transposición de la mencionada Directiva es reseñable por cuanto incorpora una disposición adicional séptima que lleva por título el de "instalación de sistemas de reconocimiento biométrico", que permite el uso de sistemas biométricos de la siguiente manera:

En virtud de lo dispuesto en el artículo 26 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, y teniendo en cuenta la Evaluación Nacional de Amenazas y Riesgos, las entidades críticas establecerán sistemas de reconocimiento biométrico de identificación o autenticación en todas o algunas de sus instalaciones con objeto de garantizar el control de accesos y el desplazamiento con fines de prevención de delitos y seguridad física. La implantación de estos sistemas, las características que deben reunir y su extensión, se regularán mediante orden del Ministro del Interior.

En la consulta formulada se hace también referencia a zonas en las que se maneja información que estaría declarada como materia clasificada, sujeta -por tanto- a la Ley 9/1968 sobre secretos oficiales. De nuevo, se trata de otra circunstancia que hay que tener en cuenta en general y en particular. La posibilidad de que hubiera materia clasificada en las instalaciones no tendría por qué aplicar a todo el recinto, sino, en todo caso, únicamente a aquellas zonas en las que se ubique y custodie tal información. Pero sin duda se trata de un referente objetivo de la necesidad general de proteger todas las instalaciones. Ello, sin perjuicio de que la evaluación de impacto y las medidas adecuadas y específicas concretasen posibilidades específicas respecto de la proporcionalidad e idoneidad en el tratamiento de datos personales para la finalidad del control de acceso a través de biometría, aspecto que por otra parte se contempla en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en su apartado 4.1.2 del Anexo II relativo a las medidas de seguridad para proteger la operación de los sistemas.

En relación con el conjunto normativo a tener en cuenta, cabe señalar que la referida Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad queda también complementada también con el Real Decreto 179/2005, de 18 de febrero, que establece normas específicas sobre la prevención de riesgos laborales en la Guardia Civil, que implica que se debe asegurar la protección de sus instalaciones y del personal que opera en ellas y que, en la práctica, se traduce en la implementación de medidas de seguridad y protocolos de actuación para la vigilancia de sus propias instalaciones al objeto de garantizar la integridad del personal y la correcta ejecución de sus funciones.

Al amplio conjunto normativo descrito cabe también añadir el Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, donde se

incluyen medidas de seguridad en instalaciones y entidades que, aunque se centra más en la seguridad privada, este reglamento complementa la normativa de seguridad pública al establecer requisitos y características que deben cumplir las empresas de seguridad y el personal que opera en el ámbito de la seguridad privada, los cuales deben colaborar con las Fuerzas y Cuerpos de Seguridad del Estado. (…).

C. El tratamiento de datos biométricos como categorías especiales de datos personales tanto para la identificación y la autenticación

Los datos biométricos son una categoría especial de datos. Las Directrices 5/2022 del Comité Europeo de Protección de Datos (CEPD), sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público (véase Versión 2.0, de 26 de abril de 2023), determinan, en su apartado 12, que el concepto de dato biométrico incluye tanto la autenticación como la identificación, y que, si bien son conceptos distintos, ambos implican el tratamiento de datos dirigidos a identificar a una persona física, por lo que constituyen tratamientos de categorías especiales conforme al artículo 9 del RGPD.

Cabe recordar que la identificación biométrica consiste en determinar la identidad de una persona comparando sus datos biométricos (por ejemplo, una huella dactilar o un patrón facial) con los datos de un conjunto amplio de personas almacenadas en una base de datos. Es decir, responde a la pregunta: ¿quién eres tú entre todos los posibles? Se trata de una operación uno-a-varios (1:N), y su principal implicación desde el punto de vista de la protección de datos es que implica una búsqueda activa dentro de un conjunto de identidades preexistentes, lo cual comporta mayores riesgos para los derechos fundamentales, especialmente en contextos de vigilancia masiva, control social o de seguridad. En cambio, la autenticación biométrica se basa en confirmar que una persona es quien dice ser, comparando sus datos biométricos con una plantilla única previamente vinculada a su identidad. Es una operación uno-a-uno (1:1), que responde a la pregunta: ¿eres tú realmente esta persona concreta? Suele utilizarse en el acceso a dispositivos o servicios.

Desde las referidas Directrices 5/2022 del CEPD y con carácter general, tanto la identificación (1:N) como la autenticación (1:1), cuando emplean datos biométricos para confirmar de forma unívoca la identidad de una persona, implica un tratamiento de "categorías especiales de datos personales" del artículo 9.1 RPGD en general y en el caso presente del artículo 13.1 Ley Orgánica 7/2021, de 26 de mayo. Ello implica la activación en general de las garantías especiales que una y otra norma confieren respecto del tratamiento de este tipo de datos especialmente protegidos. Debe especialmente tenerse en cuenta en conjunción la regulación de medidas de seguridad específicas para este tipo de tratamiento en el artículo 37.

Ahora bien, sin perjuicio de que la autenticación y la identificación supongan un tratamiento de datos especialmente protegidos, el riesgo para los derechos del interesado será menor, en función de cómo estructure el responsable el tratamiento, y sobre todo de

las medidas adecuadas y específicas que adopte. Así, la proyección concreta de estas garantías, no necesariamente habrá de serlo con la misma intensidad. No puede obviarse que -aun en el ámbito de los datos especialmente protegidos- esta distinción entre autenticación e identificación sigue siendo un elemento relevante y distintivo del impacto y riego que se genera y debe protegerse. El mismo CEPD en el apartado 17 del referido informe recuerda respecto del reconocimiento facial que:

"El reconocimiento facial basado en una plantilla almacenada en un dispositivo personal (tarjeta inteligente, teléfono inteligente, etc.) perteneciente a dicha persona, utilizada para la autenticación y el uso estrictamente personal a través de una interfaz específica, no plantea los mismos riesgos que, por ejemplo, el uso con fines de identificación, en un entorno no controlado, sin la participación activa de los interesados, en el que la plantilla de cada cara que entra en la zona de supervisión se compara con las plantillas de una amplia sección transversal de la población almacenada en una base de datos. Entre estos dos extremos existe un espectro muy variado de usos y cuestiones conexas relacionadas con la protección de los datos personales."

En consecuencia, la distinción entre identificación o autenticación y especialmente de los elementos concretos de estos tratamientos tanto por sus fines como especialmente por los medios son elementos esenciales para determinar la proporcionalidad del tratamiento, la necesidad de realizar una evaluación de impacto y la aplicabilidad de excepciones al tratamiento de datos biométricos, especialmente en ámbitos como el laboral, la seguridad pública o la prestación de servicios digitales.

Así, la identificación tiende a requerir justificaciones mucho más sólidas, siquiera sea porque un número mayor de interesados se ven afectados. No todos los tratamientos tienen la misma intensidad de impacto o requieren idénticas medidas de protección. La norma general se mantiene: la prohibición del artículo 9.1 puede exceptuarse solo mediante las circunstancias específicas del artículo 9.2, como por ejemplo el consentimiento explícito del interesado, el interés público relevante, o el que se hayan hecho manifiestamente públicos. Sin embargo, cuando se emplean datos biométricos en contextos de bajo riesgo o control restringido, el impacto sobre derechos y libertades puede ser menor, lo que influye en la proporcionalidad de las salvaguardas exigidas. Cabe mencionar expresiones de la voluntad legislativa de mantener diferencias respecto de estos tratamientos diferentes. Así, la Directiva (UE) 2024/2831 sobre trabajadores de plataformas digitales prohíbe expresamente el uso de datos biométricos con fines de identificación (1:N), es decir, mediante el cotejo de los datos de una persona con los de una base de datos de múltiples individuos. En cambio, permite la autenticación o verificación unívoca (1:1) con las garantías correspondiente a los datos especialmente protegidos cuando esta se limita a cotejar los datos del interesado con los que él mismo proporcionó previamente, siempre que el tratamiento sea lícito conforme al RGPD u otras normas aplicables (Considerando 41). Esta directiva mantiene así una distinción funcional y jurídica clara entre identificación y autenticación, reconociendo su diferente impacto sobre los derechos fundamentales el tratamiento de estos datos sensibles. En un sentido

similar, el Reglamento (UE) 2024/1684 sobre inteligencia artificial, mantiene esa distinción operativa y jurídica (considerandos 14 y ss.). En particular, el Anexo III. 1º distingue claramente entre identificación biométrica remota (varios-a-varios, M:N), considerada de alto riesgo, y verificación biométrica (uno-a-uno, 1:1), que queda expresamente excluida cuando su única finalidad es confirmar la identidad declarada por una persona. Esta distinción, de nuevo, refleja una diferencia en el nivel de impacto y riesgo sobre los derechos fundamentales.

Así las cosas y en el contexto de la normativa de protección de datos que aquí interesa, sin perjuicio de que nos encontramos ante datos especialmente protegidos del artículo 9, no todos los tratamientos basados en el artículo 9 del RGPD comportan el mismo nivel de riesgo ni exigen el mismo grado de salvaguardas. Desde una perspectiva de la legalidad y, especialmente de la proporcionalidad y evaluación de riesgos, la identificación (1:N) suele presentar mayores riesgos para los derechos y libertades fundamentales, en especial por su carácter invasivo y su tendencia a extenderse sin control en el caso de la identificación remota. En cambio, la autenticación biométrica localizada, bien diseñada y según toda una serie de circunstancias a tener en cuenta en cada caso concreto, puede ser en muchos contextos más proporcionada y menos intrusiva, especialmente si existe regulación o consentimiento libre e informado y garantías adecuadas.

Por tanto, aunque desde el plano formal ambos usos pueden estar incluidos en el artículo 9 del RGPD, el impacto real sobre los derechos y la intensidad de las medidas de protección requeridas pueden variar sustancialmente, debiendo valorarse caso por caso en función del contexto, la escala, la tecnología empleada y el control efectivo que conserve el interesado sobre sus datos biométricos.

Esta graduación en la intensidad de las garantías se refleja también en los requisitos para el levantamiento de la prohibición general de tratamiento de datos biométricos establecida en el artículo 9 del RGPD, así como en la necesidad de contar con una base jurídica adecuada conforme al artículo 6. En sentido paralelo, cabe tener en cuenta la exigencia de ley reguladora del referido artículo 13 Ley Orgánica 7/2021, de 26 de mayo, apartado 1 a). El principio de legalidad impone no sólo una base jurídica en abstracto, sino un grado suficiente de precisión y previsibilidad en función del riesgo y del impacto del tratamiento. No puede exigirse el mismo nivel de densidad normativa para una identificación masiva y automatizada sin conocimiento del afectado que para una autenticación puntual, consentida y localizada. No en vano el propio CEPD en las referidas directrices subraya la máxima exigencia de legalidad con relación a los “datos biométricos tratados con el fin de identificar de manera unívoca a una persona” (44).

Por lo que ahora corresponde, respecto del uso de sistemas biométricos por parte de las Fuerzas y Cuerpos de Seguridad cuando se empleen para la necesaria vigilancia y protección de edificios e instalaciones de los que se trata, es posible en cualquier caso acudir a la regulación actualmente existente para el uso de estos sistemas y sus correspondientes tratamientos de datos para autenticación estricta local. En el caso presente, cabe acudir al vasto conjunto normativo antes expuesto, el artículo 13 Ley

Orgánica 7/2021 y el ejercicio de poderes públicos conferidos a las Fuerzas y Cuerpos de Seguridad en la LO 2/1986.

Sin duda alguna, sería más que adecuada una acción del legislador para dotar de toda la cobertura legal y correspondientes garantías con la densidad normativa exigible en razón del impacto efectivo en el derecho de protección de datos y derechos concurrentes, tal y como ha señalado el Tribunal Constitucional (STC 292/2000) y reiteradamente esta Agencia.

De existir una regulación concreta, respecto de las garantías posibles que convendría incorporar en razón del uso concreto y de las circunstancias específicas de cada supuesto, siempre en razón de la necesidad y proporcionalidad, puede incluirse la existencia de una alternativa no biométrica, así como la previsión de mecanismos no digitales que aseguren la continuidad operativa ante situaciones de emergencia o fallo tecnológico. Podrían en su caso regularse prohibiciones específicas de tratamiento de datos biométricos en algunos supuestos, respecto de algunos colectivos de personas o con relación a algunos sistemas tecnológicos específicos y conexión con diferentes tipos de bases de datos.

La regulación podría expresar cautelas específicas respecto de tratamiento de iris, la huella dactilar y el rostro, y el registro biométrico habría de realizarse de forma asistida por personal cualificado, excluyendo procesos desasistidos o delegados en terceros. Los datos biométricos deberían permanecer bajo el control exclusivo del interesado, evitando su acceso o tratamiento por terceros, y garantizando su protección frente al fraude o la suplantación de identidad. Asimismo, se recomienda prohibir con carácter general el almacenamiento centralizado de identificadores biométricos y exigir que tanto su generación como tratamiento se realicen localmente, en sistemas aislados, sin conexión a redes ni posibilidad de interoperabilidad con otros sistemas. Los identificadores deberían ser revocables y contar con una fecha de caducidad que limite su uso al tiempo estrictamente necesario. Cada uso debería ir acompañado de información clara sobre alternativas disponibles, riesgos del tratamiento, derechos del interesado y procedimientos de destrucción de los datos.

La regulación de garantías podría incluir que los datos personales no biométricos asociados deberán conservarse solo durante 30 días y luego bloquearse. Además, los sistemas no habrían de almacenar información más allá de lo necesario para cada autenticación, ni permitir su transmisión o conservación indebida. Toda infraestructura biométrica debería instalarse en ubicaciones controladas dentro de las propias dependencias de seguridad, en condiciones que garanticen la privacidad y la seguridad técnica.

Finalmente, entre las posibles previsiones regulatorias, podría exigirse que cada sistema esté precedido de una evaluación de impacto en la protección de datos y, en su caso, una consulta previa a la autoridad de control conforme al RGPD, con actualizaciones periódicas al menos cada cuatro años o cuando se produzcan incidentes relevantes o modificaciones sustanciales del tratamiento. Además, debería garantizarse el cumplimiento del nivel alto del Esquema Nacional de Seguridad, incluyendo auditorías periódicas.

D. MEDIDAS Y GARANTÍAS DE DISEÑO DEL SISTEMA

En el caso presente y en razón de la información aportada se pone de manifiesto la existencia de suficientes garantías y medidas de diseño orientadas a evitar riesgos para los derechos y libertades de las personas físicas como, entre otros, los requisitos que se establecen con relación a los identificadores biométricos que:

- (…).
- (…).
- (…).
- (…).
- (…).
- (…).
- (…).

E. NECESIDAD Y PROPORCIONALIDAD

En cualquier caso y como se ha advertido, respecto de los espacios e instalaciones a proteger en este supuesto presente concurre una heterogeneidad de realidades diferentes. Ello exige una valoración diferenciada no solo desde la legalidad, sino especialmente desde el principio de necesidad, idoneidad y proporcionalidad, ya que no todas las instalaciones públicas vigiladas por las Fuerzas y Cuerpos de Seguridad requieren necesariamente sistemas de autenticación biométrica.

El sistema biométrico que se analiza se enmarca en un contexto especialmente sensible y regulado como es el de la protección de edificios e instalaciones concretos de la Guardia Civil, lo que confiere legitimidad al objetivo legítimo perseguido, cumpliendo así el primer requisito la necesidad en el marco del test de proporcionalidad en los términos de nuestro Tribunal Constitucional y del TJUE. El tratamiento sería idóneo (esto es, serviría para) la finalidad pretendida, que es garantizar el control de accesos para conferir una intensa seguridad, que es la necesaria para el acceso a las concretas instalaciones del ámbito de las Fuerzas y Cuerpos de Seguridad, algunas de las cuales incluso pueden albergar información clasificada o ser consideradas infraestructuras básicas, lo que en su caso refuerza el fundamento de necesidad reforzada que exige el artículo 13.1 a) Ley 7/2021 o en términos del artículo 9.2.g del RGPD, el interés público esencial. El sistema de identificación biométrica está diseñado para ser apropiado al fin perseguido, ya que el tratamiento biométrico permite verificar con mayor fiabilidad que otros mecanismos quién accede a los espacios protegidos, evita suplantaciones de identidad y permite restringir accesos no autorizados.

Bien es cierto que la documentación remitida podría haber especificado la oportunidad de mejorar los sistemas anteriores de seguridad por los que se someten a esta consulta, así como particularizar de modo más concreto las bondades y mejoras que implica el sistema elegido respecto de los anteriores u otras opciones. Como es bien sabido, la

proporcionalidad también exige que, en caso de existir varias medidas igualmente adecuadas, en el ámbito de conocimiento y decisión del responsable del tratamiento, se opte por la menos gravosa.

En términos de la reciente Sentencia del Tribunal de Justicia (Gran Sala) de de 21 de marzo de 2024, asunto C 61/22, RL y Landeshauptstadt Wiesbaden, si las medidas "se limitan a lo estrictamente necesario, en el sentido de que tales objetivos no podrían alcanzarse *razonablemente de manera igualmente eficaz*" (n. 84). Por tanto, cuando existen varias medidas eficaces, el responsable puede optar por la más eficaz, siempre que se respete la proporcionalidad y se minimicen las injerencias en los derechos fundamentales.

En cualquier caso, cabe señalar que, en el ámbito técnico, existen desarrollos recientes en tecnologías biométricas que permiten reducir significativamente el impacto sobre los derechos de los interesados, especialmente cuando se aplican condiciones como la generación local de identificadores, la no interoperabilidad, la ausencia de almacenamiento centralizado, la imposibilidad de reversión y el control exclusivo por parte del propio interesado. Estas características, recogidas en el sistema analizado, reflejan una evolución hacia esquemas de autenticación biométrica más seguros y menos intrusivos, que pueden considerarse buenas prácticas en el diseño de sistemas de control de accesos con menor impacto.

En este sentido, el sistema implantado incorpora un conjunto relevante de garantías técnicas orientadas a la minimización del impacto, con medidas como la generación local de identificadores no reversibles, su validez limitada a los períodos autorizados, el control exclusivo del interesado sobre sus datos y su no interoperabilidad. El diseño, además, limita el reconocimiento a la persona situada directamente frente a la cámara, reduciendo el riesgo de tratamientos accidentales o masivos. Estas configuraciones permiten restringir el alcance del tratamiento y previenen usos indebidos o accesos no autorizados.

Estas medidas muestran una respuesta específica y proporcional al riesgo, frente a otras medidas muy posiblemente menos eficaces, como el uso de tarjetas, contraseñas o registros manuales, que podrían ser susceptibles de pérdida, cesión o manipulación. La biometría utilizada, aplicada con este diseño específico, incrementa la eficacia del control de accesos sin recurrir a almacenamiento centralizado y con estricta vinculación entre identificador y persona autorizada. En este caso, sin embargo, las medidas alternativas —como tarjetas físicas, PINs o control presencial— puede considerarse que no ofrecerían el mismo nivel de eficacia ni garantía frente a suplantaciones, accesos indebidos o vulneraciones de seguridad, especialmente en contextos con instalaciones sensibles. Por tanto, no procede exigir su sustitución por medidas menos intrusivas si estas no alcanzaran un grado de eficacia equivalente.

También se exige la proporcionalidad en sentido estricto, que implica valorar si los perjuicios causados por la medida son desproporcionados respecto al objetivo perseguido, el sistema en cuestión incorpora numerosas garantías técnicas y organizativas que minimizan el impacto sobre los derechos de los interesados. La no centralización del

almacenamiento, la caducidad de los identificadores, la imposibilidad de reversión, la exclusividad en el uso por parte del propio interesado y el aislamiento de los terminales, evidencian un diseño que busca mitigar riesgos desde su concepción. Estas características descritas técnicamente en la documentación aportada refuerzan la evaluación positiva del sistema desde la perspectiva de proporcionalidad y minimización. Además, se plantea que en casos particulares (…) pueda evaluarse con mayor detalle la proporcionalidad en la EIPD, incluso valorando alternativas si resultaran igualmente eficaces y factibles. Esta previsión evita soluciones uniformes allí donde el impacto pudiera ser mayor.

Así las cosas, puede concluirse que el tratamiento biométrico previsto en este sistema superaría en términos genéricos para este caso adecuadamente el juicio de proporcionalidad. La existencia de un diseño orientado a la minimización de riesgos, unido a la posibilidad de modulación en determinados contextos, asegura que este tratamiento no incurre en los defectos lógicos identificados en otros enfoques que confunden necesidad con menor intrusión o que omiten el análisis técnico de idoneidad.

(…).

Según se ha expuesto, hay que partir de la intensa necesidad de protección de todo conjunto de estas instalaciones de las fuerzas y cuerpos de seguridad, si bien sería posible haber distinguido más precisamente estas necesidades de protección, así como la posibilidad de adoptar ubicaciones o medidas más concretas y adecuadas para casos específicos (…). Podría ocurrir que no resultara ni idóneo ni proporcional ni necesario, identificar biométricamente a todos (…) habiendo en su caso alternativas posibles de puntos de acceso o mecanismos de identificación excesivos. Con ser suficiente en términos generales la documentación aportada, hubiera sido más adecuado que la Evaluación de Impacto en Protección de Datos perfilara mejor si la aplicación del sistema biométrico en estas zonas (…) cumple con los requisitos de idoneidad, si no existen alternativas menos intrusivas igualmente eficaces, y si el equilibrio entre el objetivo de seguridad y los derechos afectados no se rompe por una carga desproporcionada sobre los interesados

Ahora bien, no puede obviarse la necesidad general de vigilancia en el conjunto de estas instalaciones de las fuerzas y cuerpos de seguridad y que estas particularidades sólo impliquen la posibilidad de flexibilizar en algunos casos la necesidad de identificación biométrica concreta o de en su caso brindar alguna alternativa siempre que ofrezca las mismas garantías de eficacia.

III. CONCLUSIÓN

Como resulta del art. 39.1 RGPD, el objeto de la consulta previa es proporcionar el asesoramiento al responsable previsto en el artículo 58 del RGPD cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo, esto es, en aquellos casos en los que el riesgo residual para los derechos y libertades de los ciudadanos pudiera resultar inaceptable.

En el supuesto objeto de análisis, se concluye lo siguiente:

Las medidas adoptadas en el tratamiento mitigan los riesgos suficientemente.

El tratamiento biométrico proyectado cuenta con la base legal y regulación suficiente así como cumple con los requisitos que exige el principio de proporcionalidad según la jurisprudencia del Tribunal Constitucional y el Tribunal de Justicia de la Unión Europea, al responder a un objetivo legítimo —la protección de instalaciones sensibles y la gestión de accesos en el ámbito de las competencias legalmente atribuidas a la Guardia Civil— y resultar adecuado para alcanzarlo. Las medidas técnicas adoptadas, como la generación local de identificadores no interoperables ni reversibles, su control exclusivo por el interesado, la ausencia de almacenamiento centralizado y la limitación estricta a los fines de autenticación, garantizan la idoneidad de la medida frente a otras opciones menos eficaces.

Además, la evaluación demuestra en términos razonables que no existe una alternativa igualmente eficaz que permita alcanzar los mismos fines con menor impacto. En cuanto al requisito de las garantías aplicadas —junto con la posibilidad de ajustes en espacios residenciales o de menor criticidad— permiten afirmar que los perjuicios para los derechos de los interesados no resultan desproporcionados en relación con los fines perseguidos.