Fecha: 28 de julio de 2023

DICTAMEN 1/2023

Relativo al tratamiento de categorías especiales de datos biométricos mediante el uso de dispositivos de reconocimiento facial y/o huella dactilar para el control horario del personal de un Ayuntamiento, de conformidad con la normativa de protección de datos.

1. Sobre la consulta.

Se dirige al Consejo de Transparencia y Protección de Datos de Andalucía (en adelante Consejo) una consulta, suscrita por el Delegado de Protección de Datos de un Ayuntamiento del territorio andaluz, en la que se expone la intención por parte de este de establecer un sistema de reconocimiento facial y/o con huella dactilar para el control de horario de su personal.

El consultante plantea si tal supuesto constituye un tratamiento de datos biométricos y si el mismo es lícito desde el punto de vista de la vigente normativa de protección de datos, entendiendo que, en su caso, tendrá que realizarse una Evaluación de Impacto de Protección de Datos (EIPD).

2. Naturaleza y consideración del tratamiento consultado.

Según el artículo 4.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante RGPD), se entiende por datos personales:

> *"...toda información sobre una persona física identificada o identificable ('el interesado');".*

Más concretamente, el artículo 4.14 del RGPD indica que se entienden por datos biométricos:

> *"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"*

Asimismo, el artículo 4.2 del RGPD define como tratamiento:

> *"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;"*

Por tanto, de acuerdo con los preceptos mencionados, el uso de dispositivos de reconocimiento facial y/o huella dactilar con la finalidad de un control horario implica llevar a cabo un tratamiento de datos personales, en concreto de datos biométricos, sujeto a la normativa de protección de datos.

3. Licitud del tratamiento de datos para el control de presencia y alcance del tratamiento de datos biométricos con dicha finalidad.

Entre los principios relativos al tratamiento se encuentra el de la licitud, al que se refiere el artículo 5.1 a) del RGPD, cuando enuncia que los datos personales serán tratados de manera lícita en relación con el interesado.

Por su parte, el artículo 6.1 del RGPD supedita la licitud de un tratamiento al cumplimiento de al menos una de las condiciones enumeradas en dicho artículo.

En tal sentido, puesto que el tratamiento pretendido por el Ayuntamiento responde a la finalidad, según se indica, de controlar el horario de su personal, conviene precisar que la prestación de servicios en dicha corporación local se realiza comúnmente sobre la base de una relación jurídica laboral (personal laboral) o estatutaria de naturaleza administrativa (personal funcionario/interino).

Así, la base de licitud o legitimación para el tratamiento de datos a los fines previstos de control de presencia o de jornada podría encuadrarse para ambos tipos de personal en el supuesto del artículo 6.1 b) del RGPD: *"el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales"*, el cual, como se indica en la Resolución PS/00128/2020 de la Agencia Española de Protección de Datos (AEPD), daría también cobertura al tratamiento de datos de los empleados públicos, aunque su relación no sea contractual en sentido estricto.

Al respecto, puede traerse a colación el contenido del artículo 20.3 del Estatuto de los Trabajadores (ET) sobre la potestad de adopción del empresario de la medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales.

Específicamente para el personal laboral, podría acudirse incluso a considerar la legitimación por la vía del artículo 6.1.c) del RGPD: *"el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al tratamiento"*, en conexión con el artículo 34.9 del ET que dispone la obligación para la empresa de garantizar un registro diario de jornada que deberá incluir el horario concreto de inicio y finalización de jornada de cada persona trabajadora.

No obstante lo expuesto, debe tenerse en cuenta que el artículo 9, apartado 1, del RGPD establece una regla general consistente en prohibir el tratamiento de determinadas categorías especiales de datos personales, entre los que se encuentran los *"datos biométricos dirigidos a identificar de manera unívoca a una persona física*".

En tal sentido, debe significarse que las Directrices 05/2022 del Comité Europeo de Protección de Datos (CEPD), sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público, vienen a superar en su apartado 12 la posible interpretación de que dicha prohibición solo afectaría a los

supuestos de datos biométricos dirigidos a la identificación de una persona a través de la comparación de sus datos con una o varias bases de datos que identifican a un conjunto de personas (proceso de búsqueda de correspondencia "uno a varios"), extendiéndola también a los supuestos de datos biométricos dirigidos a la autenticación o verificación de la persona con respecto al patrón previamente establecido para la misma (proceso de búsqueda de correspondencia "uno a uno"). Habida cuenta de que actualmente se trata de la interpretación que ofrece mayor seguridad jurídica, será el criterio adoptado por este Consejo.

Únicamente cabe excepcionar la anteriormente referida prohibición de tratamiento de los datos de categoría especial, cuando concurra alguna de las circunstancias que se especifican en el apartado 2 del artículo 9 del RGPD.

Por ello conviene analizar lo indicado en la letra b) del referido apartado, que excepciona la aplicación del apartado 1 cuando *"el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado"*, partiendo de la premisa de que la aplicabilidad de la excepción puede referirse también al ámbito funcionarial, tal y como expresa el informe jurídico de la AEPD 0002/2022 al afirmar que: *"aunque la función pública no se rige, en puridad, por normas laborales sino por el derecho administrativo estatutario de los funcionarios públicos, la interpretación que de ella se deriva, comparte, en términos generales, la misma naturaleza jurídica"*.

A su vez, cabe indicar que la mención a la autorización por el Derecho de los estados miembros de la UE debe entenderse referida, en el caso del Estado Español, a la existencia de una norma previsora de rango legal en consonancia con lo dispuesto en el artículo 53.1 de la Constitución Española, por tratarse del desarrollo de un derecho, el de la protección de datos, reconocido como fundamental. Abundando al respecto, la sentencia del Tribunal Constitucional 76/2019, de 22 de mayo, precisa que la norma legal debe reunir todas las características indispensables como garantía de la seguridad jurídica, expresando todos y cada uno de los presupuestos y condiciones de la intervención, de forma que las limitaciones del derecho fundamental establecidas por una ley pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad.

Ello supone, como bien apunta el Dictamen 2/2022, de la Autoridad Catalana de Protección de Datos, que *"la afectación por el derecho a la protección de datos que se derive de la norma debe ser previsible"* y que *"no se puede considerar previsible la norma si no concreta la posibilidad de utilizar datos biométricos con el fin de realizar el control horario"*.

Al hilo de lo indicado, puede afirmarse que en la actual normativa legal española no se contiene autorización alguna para considerar necesario el tratamiento de datos biométricos con la finalidad de un control horario de la jornada de trabajo: ni para el personal laboral, puesto que los artículos 20.3 y 34.9 del ET a los que se ha hecho referencia no contienen tal autorización, ni para el personal sometido a una relación jurídica administrativa al no constituirse en necesaria habilitación la previsión relacionada con el

cumplimento de jornada y horario a la que alude el artículo 54.2 del Real Decreto Legislativo que aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público (EBEP).

No obstante, a falta de previsión legal, la referida autorización o habilitación, de acuerdo con lo indicado en el artículo 9.2 b) del RGPD, podría estar prevista en los convenios colectivos para el personal laboral y en los acuerdos sobre condiciones de trabajo del personal funcionario en el marco de la negociación colectiva (en este último supuesto con los requisitos que para su eficacia se recogen en el artículo 38.3 del EBEP), siempre con el establecimiento de las garantías adecuadas respecto a los derechos fundamentales y de los intereses de los afectados.

Completando lo expuesto, también podría considerarse el levantamiento de la prohibición del tratamiento de datos biométricos por concurrencia de la prestación del consentimiento explícito por parte del interesado para el tratamiento de dichos datos personales con uno o más de los fines especificados (salvo establecimiento expreso contrario a tal sentido por parte del derecho de la Unión o de sus estados miembros), según se establece en el artículo 9.2 a) del RGPD.

Eso sí, debe precisarse al respecto que el artículo 4.11 del RGPD se refiere al consentimiento del interesado como *"toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen"*. Las condiciones para su consideración se prevén en el artículo 7 del RGPD, pudiendo acudirse también a las Directrices 5/2020 del CEPD, sobre el consentimiento en el sentido del RGPD.

Además, siguiendo la línea de argumentación del Dictamen 1/2022 emitido por este Consejo: *"El consentimiento como base legitimadora se asienta en una invitación previa del responsable al interesado para que acepte una operación de tratamiento. La invitación y su respuesta, al poder constituirse como una excepción a la prohibición de tratamiento de categorías especiales de datos, y afectar por tanto a un derecho fundamental, debe cumplir todos los requisitos previstos específicamente para ello"*.

También precisa el mencionado Dictamen que el consentimiento como base legitimadora requiere asimismo una manifestación de voluntad libre, una libre expresión que *"se asocia a libertad de elección, prestar o no prestar el consentimiento y el control real del interesado"*, descartando la existencia de algún tipo de coacción. Igualmente, indica que la situación de desequilibrio entre el interesado y las Administraciones Públicas responsable del tratamiento, lleva a la consideración de que *"el consentimiento no es la base legitimadora en principio más apropiada de tratamiento por las Administraciones Públicas de los datos personales"* [...] *debiendo analizarse con cautela cuando no estuviese al menos previsto por la norma aplicable"*. Finalmente debe evaluarse si su prestación o no prestación *"puede depararle al interesado algún tipo de perjuicio o ha de producir algún tipo efecto desfavorable que condicione precisamente la libertad con la que ha de ser emitido"*.

Trasladado esto al supuesto que nos ocupa, únicamente podría considerarse la existencia de un consentimiento libre si el interesado dispone de una alternativa de libre elección para cumplir con el control horario o de presencia, es decir, en expresión del propio Dictamen 1/2022: *"para que dicho consentimiento se considere otorgado libremente han de habilitarse alternativas de modo que pueda atenderse a los interesados sin que se tenga que realizar un tratamiento de sus datos biométricos"*.

Además, el consentimiento deberá ser informado (principio de transparencia del articulo 5.1 a) del RGPD), inequívoco (Considerando 32 del RGPD), y demostrable por el responsable del tratamiento (artículo 7.1 del RGPD).

4. Principios, obligaciones y recomendaciones en relación con el tratamiento de datos biométricos para el control de presencia.

El tratamiento, de producirse, deberá cumplir también con el resto de principios y obligaciones derivados de la normativa de protección de datos, entre los que conviene destacar el de minimización (artículo 5.1 c) del RGPD).

En concreto, el Dictamen 3/2012 del Grupo de Trabajo del artículo 29, sobre la evolución de tecnologías biométricas, afirma lo siguiente en relación con el análisis del cumplimiento del principio de minimización:

> *"Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no sólo lo más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar. Un tercer aspecto a ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado."*

Por otra parte, se enumeran a continuación una serie de directrices y recomendaciones de conveniente cumplimiento, cuya práctica totalidad figuran recogidas en el anteriormente referido Dictamen 3/2012:

-El trabajador debe ser informado sobre el tratamiento.

-El principios de limitación de la finalidad deber respetarse junto con los demás principios de protección de datos: especialmente, los de necesidad, proporcionalidad y minimización de datos.

-En todo caso, el tratamiento también deberá ser adecuado, pertinente y no excesivo en relación con dicha finalidad. Por tanto, los datos biométricos que no sean necesarios para esa finalidad deben suprimirse y no siempre se justificará la creación de una base de datos biométricos.

-Los datos biométricos deberán almacenarse como plantillas biométricas siempre que sea posible. La plantilla deberá extraerse de una manera que sea específica para el sistema biométrico en cuestión y no utilizada por otros responsables del tratamiento de sistemas similares a fin de garantizar que una persona solo pueda ser identificada en los sistemas biométricos que cuenten con una base jurídica para esta operación.

-El sistema biométrico utilizado y las medidas de seguridad elegidas deberán asegurarse de que es imposible o al menos rastreable la reutilización de los datos biométricos en cuestión para otra finalidad.

-Deberán utilizarse mecanismos basados en tecnologías de cifrado, a fin de evitar la lectura, copia, modificación o supresión no autorizadas de datos biométricos.

-Los sistemas biométricos deberán diseñarse de modo que se pueda revocar el vínculo de identidad.

-Deberá optarse por utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.

-Los datos biométricos deben ser suprimidos cuando no se vinculen a la finalidad que motivó su tratamiento y, si fuera posible, deben implantarse mecanismos automatizados de supresión de datos.

5. Realización de Evaluación de Impacto relativa a la protección de datos (EIPD).

Tal y como se apunta en la consulta, un tratamiento como el indicado requerirá la realización previa, por parte del responsable del tratamiento, de la evaluación de impacto relativa a la protección de datos establecida en el artículo 35 del RGPD, habida cuenta del cumplimiento de los criterios correspondientes a los números 4, 5 y 10, del documento *"Listas de tipos de tratamiento de datos que requieren evaluación de impacto relativa a protección de datos"*, hecho público por la AEPD y este Consejo en desarrollo de la previsión contemplada en el apartado cuarto del referido artículo 35.

6. Conclusiones.

a) El uso de dispositivos de reconocimiento facial y/o huella dactilar con la finalidad de un control horario del personal de un Ayuntamiento implica un tratamiento de datos personales biométricos, sujeto a la normativa de protección de datos.

b) La base de legitimación para el tratamiento de datos con la finalidad de controlar la presencia o la jornada laboral del personal del Ayuntamiento podría encontrarse en el artículo 6.1 b) del RGPD y también en el artículo 6.1 c) del RGDP, este último exclusivamente para el personal laboral.

c) Los datos biométricos son una categoría especial de datos personales, por lo que su tratamiento debe considerarse, en principio prohibido, conforme a lo dispuesto en el artículo 9.1 del RGDP.

d) El levantamiento de la referida prohibición no puede ampararse en la actualidad en la concurrencia de la circunstancia prevista en el artículo 9.2 b) del RGPD puesto que en la actual normativa legal española no se contiene autorización para considerar necesario el tratamiento de datos biométricos con la finalidad de un control horario de la jornada de trabajo. A falta de tal previsión legal, la referida autorización o habilitación podría preverse en los convenios colectivos para el personal laboral y en los acuerdos sobre condiciones de trabajo del personal funcionario en el marco de la negociación colectiva con los requisitos previstos para su eficacia.

e) El levantamiento de la prohibición basada en la concurrencia de la circunstancia del consentimiento explícito del interesado prevista en el artículo 9.2.a), debe analizarse con cautela ante la situación de desequilibrio entre dicho interesado y la Administración Pública responsable del tratamiento. Podría

considerarse únicamente si se dispone de una alternativa de libre elección para cumplir el control horario o de presencia y si el consentimiento es informado, inequívoco y demostrable por el responsable del tratamiento.

f) El tratamiento de datos biométricos con la finalidad de control de presencia deberá cumplir con el resto de principios y obligaciones derivados de la normativa de protección de datos, destacando el de minimización (artículo 5.1 c) del RGPD) y seguir las directrices y recomendaciones recogidas en el Dictamen 3/2012 Grupo de Trabajo del artículo 29.

g) El responsable del tratamiento de datos biométricos con la finalidad de control de presencia realizará antes del tratamiento la evaluación del impacto relativa a la protección de datos establecida en el artículo 35 del RGPD.

EL DIRECTOR DEL CONSEJO DE TRANSPARENCIA
Y PROTECCIÓN DE DATOS DE ANDALUCÍA

Jesús Jiménez López.