- **Expediente N.º: PS/00218/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: RECLAMANTE (figura en ANEXO GENERAL) (en adelante, la parte reclamante), con fecha 22/06/2020, presenta reclamación ante la AEPD. La reclamación se dirige contra **ENTIDAD URBANÍSTICA COLABORADORA DE CONSERVACIÓN EUROVILLAS,** con NIF G79414033, en calle ******DIRECCIÓN.1***, Madrid (en adelante, la parte reclamada). Los motivos en que basa la reclamación son que la reclamada instauró un sistema de registro diario de jornada laboral de los empleados a través de técnica de reconocimiento facial (RF).

Manifiesta:

-El 13/02/2020, la reclamada instaló en los lugares de trabajo un sistema de registro horario "*por huella dactilar*", modificando el previo de uso de tarjeta. La representación de los empleados envió un escrito el 17/02/2020, del que acompaña copia como DOCUMENTO 1, firmado por la reclamante y otros dos empleados, como "*Delegados* ***XXXXXXXXXX***", en el que mencionan que no se da en su totalidad el cumplimiento del artículo 9.2.b) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27/04/2016, 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 (en lo sucesivo, RGPD); y que se ha tomado la medida sin haber comunicado ni negociado con los representantes de los trabajadores, solicitando que se cambie a otros sistemas.

-Con fecha 17/02/2020, la reclamada hizo entrega en mano de una comunicación del sistema implantado de "*reconocimiento táctil*", con indicación de puesta en marcha el 1/03/2020.

-En escrito de la reclamada de la misma fecha, 17/02/2020, contestó al de la reclamante de 17/02 indicando que " *no existe obligación de obtener el consentimiento dado que el sistema de fichaje implantado persigue unos intereses legítimos por parte de la empresa*", "*dado que la legislación laboral obliga a registrar el número de horas que realizan los trabajadores*", y que "*el uso de las tarjetas que se venia utilizando provocaba fraudes en la gestión y por tanto no eran medios adecuados a la finalidad perseguida*". Acompaña DOCUMENTO 3 con el recibí, que verifica estas afirmaciones.

-Se dirigió escrito por la reclamante a la reclamada el 11/03/2020, solicitando:

"Características del tratamiento, forma de almacenamiento y responsable de la custodia, forma en que van a estar disponibles los registros de jornada, tanto para trabajadores como para sus representantes."

Acompaña DOCUMENTO 4 que contiene la respuesta de 12/03/2020, indicando que la responsable de los datos es la persona nombrada por la empresa para tratar los datos de los trabajadores y que debido a la situación creada por el "*coronavirus*", se está valorando el cambiar el sistema de registro de horas actual, "*por uno de vectores faciales, en cuyo caso, almacenaría una fotografía, al igual que el sistema que se utilizaba con las tarjetas anteriores*".

-Manifiesta la reclamante, que en fecha 30/04/2020, la reclamada comunica un cambio en el sistema de registros horarios originado por la enfermedad COVID-19 y que va a implantarse a partir del 6/05/2020. Consiste en la identificación del personal por datos de su propio rostro, "*mediante vectorización facial*" "*Este sistema funciona a partir de la identificación de un porcentaje de características extraídas del rostro, sin tomar una imagen en tres dimensiones de las caras "entendemos que esta medida es menos invasiva que la grabación del momento del fichaje por cámara, que además suponía el contacto físico con un lector de tarjeta compartido. El fin único de estos datos es el fichaje de personal y análisis de los tiempos de trabajo para el cumplimiento del decreto ley 8/2019, con objeto de analizar los datos en toma de decisiones y la defensa de sus interese legítimos". "Estos datos se encontrarán en los servidores de esta entidad, en ningún caso en la nube*". Acompaña DOCUMENTO 6.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), el 7/07/2020, se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de:

"*1.La decisión adoptada a propósito de esta reclamación.*
2. Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.
3. Análisis de Riesgos y Estudio de Evaluación de Impacto relativos al tratamiento de datos personales objeto de la reclamación.
4. Base de legitimación de dicho tratamiento y justificación.
5. Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia.
6. Cualquier otra que considere relevante."

Con fecha 5/08/2020, se recibe en esta Agencia escrito de respuesta indicando:

1) Es un "*ente administrativo*" "*dependiente de*" la Comunidad de Madrid si bien con personalidad jurídica propia y plena capacidad de autonomía para el cumplimiento de sus fines, de conformidad con la ley y los Estatutos, y que fundamentalmente consisten en la conservación de los espacios libres de dominio y uso público, y en su caso de los privados, y el mantenimiento de las dotaciones como instalaciones e infraestructuras de la urbanización.

El carácter de "*entidad administrativa*" se recoge de forma expresa, el artículo 26.1 del Real Decreto 3288/1978, de 25/08, por el que se aprueba el Reglamento de Gestión Urbanística para el desarrollo y aplicación de la Ley sobre Régimen del Suelo y Ordenación Urbana (RGU) "*las entidades urbanísticas colaboradoras tendrán carácter administrativo y dependerán en este orden de la administración urbanística actuante*".

Aporta copia de sus Estatutos, cuya versión vigente aparece publicada en el BOCM de 29/05/2014. Se consideran de importancia para el caso, las siguientes disposiciones:

“art 1- *Se constituye una entidad urbanística colaboradora de naturaleza administrativa con personalidad jurídica propia y plena capacidad legal desde su inscripción en el registro de entidades urbanísticas colaboradoras de la Consejería competente en materia urbanística de la Comunidad de Madrid*.”

Esta entidad de conservación se constituyó con carácter obligatorio en virtud de las determinaciones del plan especial ciudad de las Américas, hoy Euro Villas, aprobado definitivamente el 23 de marzo de 1988 y estará compuesta por todos los propietarios comprendidos en su ámbito territorial.

La entidad de conservación se regirá por lo dispuesto en los presentes estatutos y en lo no previsto por ellos por los artículos 24 a 30 y 68 a 70 del RGU de 25 de agosto de 1978 y demás disposiciones concordantes y complementarias.

“Artículo 3, objeto: Esta entidad tiene por objeto la conservación de la obra urbanizada, de los espacios libres de dominio y uso público y, en su caso, de los privados y el mantenimiento de las dotaciones e instalaciones de los servicios urbanísticos e infraestructuras conforme a lo dispuesto en el artículo 32 de estos estatutos.”

En el artículo 4 se indican los fines básicamente de ejecución de obras necesarias para la reparación y mantenimiento cuya conservación sea necesaria en cuanto al uso y utilización de los bienes y servicios.

En el artículo 5 se establece: “A l*a Consejería competente en materia urbanística como administración actuante le corresponden las siguientes funciones: aprobar el texto de los estatutos para la constitución de la entidad de conservación, aprobar la constitución de la entidad de conservación para su inscripción en el registro. En el apartado c se indica que sin perjuicio de que la administración actuante sea la Consejería de Obras Públicas y Urbanismo y Transporte, corresponderá a los Ayuntamientos en los que se encuentra ubicada la urbanización, la utilización de la vía de apremio para el cobro de las cantidades adeudadas por cualquiera de los miembros de la Entidad de Conservación. En el apartado d) indica que corresponde a la administración actuante resolver los recursos de alzada contra acuerdos de la entidad, así como acordar la disolución de la entidad en los supuestos contemplados en el artículo 40 de los estatutos y cuantas otras atribuciones resulten de la legislación urbanística y autonómica*.”

El artículo 19 prevé como facultades y funciones del Consejo Rector, el nombramiento y separación del personal y señalamiento de su régimen de trabajo y la administración de la entidad.

2) La entidad cuenta con equipamientos, maquinaria y personal propio para acometer sus tareas de conservación y mantenimiento de las infraestructuras y el dominio público de la organización. “*Agrupa a unos 4.000 propietarios de parcelas sobre las que existen construidas alrededor de unas 3.000 viviendas unifamiliares que son habitadas por una población superior a los 10.000 habitantes*.”

En la actualidad, la plantilla está formada por 38 trabajadores que prestan sus servicios en algunos casos en régimen de turnos, contándose con servicios de urgencias que cubren una atención de 24 horas al día. La revisión de este personal y la comprobación de su asistencia al puesto de trabajo siempre ha sido objeto de control. “*Hace unos años se fichaba*”, luego se

hizo uso de tarjetas individuales, pero al detectarse fraudes con las tarjetas que se dejaban a otros empleados, "*se estableció un sistema de fichado*" por medio de huella dactilar y posteriormente por los riesgos del COVID-19, se varió el sistema al RF.

3) "*El registro de las jornadas de trabajo es obligatorio para la empresa en virtud del artículo 34.9 del Estatuto de los trabajadores*". "*Dado el derecho y a la vez la obligación que tiene la Entidad de llevar un control y registro de la jornada de los trabajadores que sea fidedigno, el sistema implantado es efectivo y proporcional, a la vez que el más adecuado para garantizar la salud de los trabajadores, en estos tiempos de pandemia*." "*La base de legitimación para el tratamiento de estos datos viene dada por el contrato laboral existente con los usuarios (art. 6.1.b RGPD); la obligación legal de llevar acabo un registro de la jornada laboral de los empleados de la Entidad (art. 6.1.c) y la propia necesidad de la empresa de controlar a los trabajadores (art. 6.1. f), de modo que la propia Entidad pueda prestar las funciones de interés público que tiene encomendadas dado su carácter de administración pública (art. 6. 1.e*)."

4) Los sistemas empleados por la entidad en ningún caso conservan imágenes o fotografías de la huella dactilar o rostro de la persona, sino que son sistemas biométricos en los que para su funcionamiento no utilizan imágenes de huellas o rostros, sino meras descripciones de estos que se traducen en las tomas de varias minucias o patrones del dibujo de la huella del rostro. Por tanto, el sistema solo toma unas pocas minucias o características especiales concretas, en general la posición o dimensiones, elementos de la huella o el rostro fundamentalmente, que no permiten reconstruir a partir de ellas la huella ni el rostro de una persona, por lo que consideran que no permiten la identificación inequívoca del sujeto más que dentro de un grupo reducido de personas como es el personal de la entidad. "*El sistema está instalado en un ordenador independiente, protegido bajo contraseña, al que solo tiene acceso una persona y que los datos biométricos estadísticos, quedan encriptados, no son extraíbles, ni conocibles, por formar parte del propio programa, sin que se puedan usar para ninguna otra finalidad*." Entiende que está actuando en todo momento conforme a derecho.

TERCERO: Con fecha 4/09/2020, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 58.1 del RGPD, de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Solicitó a la reclamada que aportar el análisis de riesgos, la evaluación de impacto del tratamiento del dato biométrico y características del sistema.

Con fecha de 29/10/2020, se respondió, que "*ya se contestó sobre esta reclamación en el seno del procedimiento de traslado y admisión de la reclamación*."

QUINTO: Con fecha 2/09/2021, se acordó por la Directora de la AEPD:

"*INICIAR PROCEDIMIENTO SANCIONADOR a* **ENTIDAD URBANÍSTICA COLABORADORA DE CONSERVACIÓN EUROVILLAS***, con NIF G79414033, por la presunta infracción:*

-Del artículo 9.2.b) en relación con el 6.1 del RGPD, tipificada en el artículo 83.5.a) del RGPD

-Del artículo 35 del RGPD, tipificada en el artículo 83.4.a) del RGPD."

(…)

"*QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP) , las sanciones que pudieran corresponder serían de multas de 100.000 euros, y de 20 mil euros, según lo especificado, sin perjuicio de lo que resulte de la instrucción*."

SEXTO: Con fecha 17/09/2021, se reciben alegaciones en las que la reclamada manifiesta:

1- Se considera incluida en el apartado d) del artículo 77.1 de la LOPDGDD como "*organismo público y entidad de derecho público vinculada o dependiente de las administraciones públicas",* por lo que procedería en su caso una sanción de apercibimiento. Considera, además, que es indiferente si el ente público está realizando o no una actividad pública, porque la normativa regula la posibilidad de sancionar por lo que se es, una administración pública, y no por la actividad que se realiza. El citado artículo señala que las " *Administraciones Públicas serán sancionadas con apercibimiento por el mero hecho de serlo, y siempre que reúnan esa condición, sin que el ordenamiento establezca que ello solo ocurrirá cuando realicen funciones públicas, lo que es una interpretación expansiva, o más bien, una creación legal "ex novo" de esa Agencia, dado que carece de soporte legal alguno y no existe norma que dé pie, siquiera a esa interpretación, sin que por otro lado, las infracciones de que se acusa a la Entidad puedan considerarse como de derecho privado."*

Es indiferente que la contratación laboral de los trabajadores de la entidad sea de carácter privado. Indica que carece de sentido separar a que ámbitos puede afectar la actividad, dada la razón de ser administrativa del propio ente y sus funciones públicas que realiza. No se está ante una cuestión de índole laboral, sino "*ante una cuestión de protección de datos, materia que compete ser cumplida por el ente administrativo en el ejercicio de su actividad pública y con la intervención de sus órganos rectores de funcionamiento, cuya actividad está sujeta a derecho administrativo*."

Las decisiones relacionadas con despidos, organización del personal, y cualquier cuestión laboral, se adoptan por el Consejo Rector, estando todas estas cuestiones sometidas al derecho administrativo, y pudiendo impugnarse en alzada ante la CCAA de Madrid o en vía contenciosa (art 38 de los Estatutos). "*La situación es similar a lo que ocurre con las reclamaciones de propietarios morosos de la entidad, en las que el Tribunal Supremo ha dicho que solo es competente para su conocimiento en la jurisdicción contencioso-administrativa"*. Como por ejemplo, el auto de 30/05/2012, recurso 203/2009. Señala que incluso cuando los empleados demandan laboralmente a la entidad, dado el carácter de administración pública de la misma, no tienen que realizar actos de conciliación previa señalados en los artículos 63 y 64 en relación con el 69.1 de la ley de la jurisdicción social, lo

que demuestra que no es una relación privada la que existe con dichos empleados de la entidad.

2- "*La iniciación del procedimiento sancionador, lo es por el sistema de reconocimiento facial, implantado según esa Agencia, desde el 6 de mayo de 2021. Con ello, se está reconociendo la validez del sistema de reconocimiento mediante huella dactilar que anteriormente había implantado la Entidad*." "*Es por lo tanto, el cambio del sistema, de reconocimiento de huella dactilar a facial, lo que generaría las infracciones que se atribuyen a la Entidad*." Considera que si la huella toma las minucias, en el RF, se hace sobre el rostro, siendo en ambos casos lo mismo, no sirven para identificar de forma univoca a una persona. No se trata de datos de carácter especial pues no se conservan imágenes o fotografías del rostro, que para su funcionamiento utilizan "*meras descripciones de estos*", "*patrones de dibujo del rostro*", posición o dimensiones de elementos que no permiten reconstruir a partir de ellas el rostro de una persona, "*las cuales además podrían coincidir en otras muchas personas, por lo que no permiten la identificación inequívoca del sujeto, mas que dentro de un grupo reducido de personas, como es el personal de la entidad*". Los datos almacenados en un ordenador, son solo accesibles a una persona, quedando encriptados y cifrados. Considera que no seria de aplicación la prohibición del artículo 9.1 del RGPD pues "*no se esta antes datos biométricos dirigidos a identificar de manera inequívoca a una persona física*."

Por tanto, no siendo datos de carácter especial, no es preceptivo aportar la Evaluación de Impacto establecida en el artículo 35 del RGPD.

3-La principal causa y contexto que motivó el cambio de un sistema de registro horario por huella dactilar a uno de RF, se debió a la extraordinaria y grave situación derivada de la alerta sanitaria por la pandemia*, "que pone en peligro la salud e incluso la vida de los trabajadores de la Entidad, y con ello, que la Entidad pueda cumplir sus fines y obligaciones." Las tareas que desempeña su personal afectan a la salud pública-limpieza , vadeo de calles, mantenimiento de red de saneamiento, alumbrado etc., junto con desinsectación que afectaba a 10.000 residentes, que en aquellas fechas salían de un confinamiento.* Se pretendía no tocar el lector de huellas y poner su dedo en el sensor. Considera proporcional el sistema al ser un sistema fidedigno y efectivo, y el más adecuado para garantizar la salud de los empleados.

4- Considera que la base de legitimación del tratamiento viene dada por

-"*El contrato laboral con los usuarios, art 6.1.b) del RGPD*

- La obligación legal de llevar a cabo un registro de la jornada laboral de los empleados de la entidad, art 6.1.c) del RGPD

-la propia necesidad de la empresa de controlar a los trabajadores (art. 6.1. f), de modo que la propia Entidad pueda prestar las funciones de interés público que tiene encomendadas, dado su carácter de administración pública (art. 6. 1.e)."

5- "*Con la mejora de la situación epidemiológica se ha vuelto al sistema de fichaje por tarjeta, si bien se está negociando al respecto*"

6- En el acuerdo, se analiza como única posibilidad de legalidad del tratamiento, la laboral, contemplada en la letra 2.b) del artículo 9 del RGPD, concluyéndose que no procede por tres cuestiones:

a) Se dice, que no se justifica que el tratamiento a través del RF **sea necesario** para el cumplimiento de las obligaciones en materia laboral como lo es el registro de jornada y ello porque ese control ya se había realizado previamente con el sistema de tarjetas. Considera dicho cambio de sistema necesario pues las tarjetas se prestaban por unos empleados a otros.

b) Las letras g) y h) del artículo 9.2 del RGPD, por si solas, de forma individual, y más puestas en relación entre ellas, con la propia letra b), justificarían el tratamiento especial, dada la extraordinaria situación de pandemia que hemos vivido y que se ha expuesto. La letra g) habilita en el supuesto de que sea "*necesario para fines de interés publico esencial*", siendo evitar la propagación del COVID un interés publico esencial, con recomendaciones para que no hubiera contacto interpersonal ni contacto con superficies. También considera que la letra h) habilita mejor el tratamiento, "*es necesario para fines de medicina preventiva o laboral*", siendo esa la finalidad que ha movido el cambio del sistema de registros horarios, evitar los contagios entre el personal laboral de la entidad.

7- Se dice que no se respetó la negociación o consulta con los representantes del personal, pero esto no fue así, pues se informó, se negoció y finalmente se optó por el mantenimiento del registro facial mientras duraba la pandemia, debiendo destacarse además que "*los representantes de los trabajadores no quisieron nunca formular una reclamación ante la AEPD, sino simplemente realizar una consulta*".

8- La reclamada es una entidad que presta servicio publico, sin animo de lucro. Actuó con animo de proteger la salud de su personal, con el fin de garantizar que pudiera prestar su servicio que califica de esencial durante el confinamiento, entre un personal, al que le afectó de manera alta el contagio de la enfermedad. Por todo ello, considera que no puede considerar culpable a la reclamada. Añade, que además la sanción es desproporcionada, por:

a) en la infracción del artículo 9.2.b) en relación con el 6.1 del RGPD, considera que no se pueden producir las agravantes:

- del 83.2.a) del RGPD, pues la infracción es ya de carácter muy grave, "*no puede utilizarse esa misma gravedad intrínseca en la propia infracción para añadir a la misma un agravante*" "*Se esta sancionando dos veces por la misma conducta*".

-del 83.2. b) del RGPD por el mismo motivo, la negligencia ya va incorporada en el tipo que se sanciona, suponiendo una ficticia suma de agravamientos que no procede.

-del artículo 76.2.b) de la LOPDGDD, no lo considera relevante, pues no es una entidad con gran experiencia en el tratamiento de datos con estas especiales características.

-del artículo 83.2.k) del RGPD, siendo de nuevo una agravante ya incluida en la sanción como muy grave, no contemplando la causa que se manifiesta como agravante el citado artículo

b) En la infracción del artículo 35 del RGPD, algunas de las cuestiones que se señala como agravantes de la infracción, estarían ya incorporadas en esta misma infracción, nuevamente

se están castigando dos veces, por lo que seria la misma conducta o reproche sancionador y en concreto, considera que no se pueden producir las agravantes por:

-el artículo 83.2.b) por un grado cualificado de grado de diligencia, al no contemplar algún tipo de análisis sobre el tratamiento, que se mantiene durante la tramitación del traslado, continuando la realización del tratamiento (93.2.1 del RGPD). "*si lo que se castiga es no haber realizado una valoración de impacto, porque se considera que antes de implantar un sistema de reconocimiento facial, que esta debe realizarse, no puede considerarse agravante no haber hecho el análisis o la propia evaluación".*

Considera se debería valorar, como atenuantes:

- La situación de grave emergencia sanitaria nacional y excepcionalidad (con estados de alarma) derivada de la pandemia vivida. No puede obviarse que estamos hablando del mes de mayo de 2020, pleno estado de alarma con situación de confinamiento domiciliario. La pretensión última y que motiva el cambio de sistema a RF fue la lucha contra la pandemia y garantizar o cuando menos disminuir las posibilidades de contagio de la plantilla.

Considera que las sanciones ni siquiera guardan la debida proporción entre ellas mismas:

Se proponen de 100.000,00 euros y 20.000,00 euros. El artículo 83.5.a) del RGPD, aplicable a la primera infracción, hace alusión al 4 % del volumen de negocio en el caso de empresas y con un máximo total posible de 20 millones de euros, mientras que en el 83.4 del RGPD aplicable a las sanciones graves, este porcentaje se reduce al 2 % con un máximo de 10 millones de euros. Dado que una sanción es muy grave, debería ser el doble de una grave, sin embargo la sanción muy grave es cinco veces la grave, alcanzando los 100.000,00 euros cuando el doble de la grave serían 40.000,00 euros.

Teniendo en cuenta que se trata de un ente administrativo carente de lucro, debe reducirse a como mínimo una cuarta parte, situándose entre los 25.000,00 euros para la muy grave y los 12.500,00 euros para la grave, si bien, esto se dice con un carácter subsidiario, dado que ni hay infracción, ni de haberla, se puede sancionar económicamente, siendo lo correcto hacerlo con apercibimiento.

SÉPTIMO: Con fecha 21/03/2022, se inicia un periodo de practica de pruebas, dando por reproducidos a efectos probatorios la reclamación interpuesta y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones previas de investigación que forman parte del procedimiento E/08378/2020. Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por la reclamada y la documentación que a ellas acompaña.

Además, se solicita a la reclamada que aporte e informe:

a) Sistema que está utilizando actualmente para el control de jornada laboral, y si dejó de usar el RF, fecha y acreditación de ello.

Con fecha 4/04/2022, se recibe respuesta de la reclamada en la que indica que "*el sistema actual empleado*" es el de tarjetas, desde que recibió el acuerdo de inicio por "*prudencia*" se suspendió el sistema de RF el 8/09/2021, en cuanto adquirieron las tarjetas. Aporta factura de adquisición de 40 tarjetas de 6/09/2021, tipo "*proximidad por radiofrecuencia RFID PAS*".

b) En el escrito de la reclamada de 12/03/2020 dice que "*Se está valorando cambiar el sistema de registro de horas actual por uno de vectores faciales, en cuyo caso almacenaría una fotografía al igual que el sistema que se utilizaba con las tarjetas*". Explique el sentido y finalidad de lo subrayado dentro del sistema de RF implantado.

Manifiesta que lo que quiere decir es que "*no hay variaciones significativas entre el sistema de tarjetas y el de vectores faciales, siendo la finalidad explicárselo a los delegados* ***XXXXXXXXXX****. En cualquier caso, en ese escrito solo se hacía referencia a una posibilidad que se estaba barajando. por lo que cuando se redacta no se conoce todavía en qué consiste realmente el sistema*".

c) Si la recogida de imágenes del rostro para el registro se efectuó con imágenes (fotografías) de los empleados previamente usadas, o con actuación presencial de los empleados.

Manifiesta que con actuación presencial. "*El mismo equipo que hace el reconocimiento, captura previamente para ello los vectores que va a emplear sobre el propio empleado. Los datos o minutas faciales, se captan, entran, se cifran, son usados por el aparato y no salen del mismo, sin que puedan usarse para ningún otro fin, ni extraerse. El aparato solo reporta externamente a un único equipo informático de la entidad: el día, hora y nombre de la persona verificada*".

d) Identificación del soporte tecnológico adquirido para el funcionamiento técnico del sistema y en que consiste. Añadiendo los elementos que lo componen, y si se contrató los servicios de la gestión del sistema con un proveedor. Si el sistema cuenta con alguna certificación tipo ISO sobre datos biométricos. Copia del contrato de gestión de tratamiento de datos por encargo.

Manifiesta que se adquirió "*un sistema completo, una unidad compacta, maquina lectora y que procesa la información y que lleva su programa propio*". "*El proveedor no tiene acceso ni se contrató para gestionar nada del sistema*".

En la factura que aporta documento 2, figura: 31/03/2020, equipo por importe de 375 euros "*equipo de control presencial y acceso facial SAFIER, VSFTCT2MTFN3A* "*SOFTWARE GESTIÓN PRESENCIAL SAFIRE CONTROL CENTER*" de fabricación china, modelo SF-AC3062KEMR-IP según el folleto que adjunta en documento 4 en que se ve el dispositivo, y el literal:

"*control de accesos y presencia- Reconocimiento facial y tarjeta EM-1.600 caras, 2.500 tarjetas y 50.000 registros, comunicación TCP/IP, USB y WIFI, controladora integrada, Software SAFIRE CONTROL CENTER AC, Lector biométrico autónomo de control de accesos*."

Se acompaña como parte del folleto también el literal "especificaciones" que describe una descripción de elementos.

Se acompaña con el folleto la imagen del dispositivo "HIKVISION", "DS-K1T9105 Series terminal de reconocimiento facial que informa que funciona con algoritmo de aprendizaje puede funcionar como múltiples modo de autenticación 1:N emparejamiento de cara, IC autenticación tarjeta, etc. También indica las "*características*"

Con fecha 26/04/2022 se busca en GOOGLE “SAFIRE CONTROL CENTER AC SOFTWARE existiendo entre otras la dirección:

“*Safire Control Center AC Software*

https://svtclti.com › manuales › SAFIRE-HIKVISION”, en la que pinchando sale el “*manual usuario SAFIRE CONTROL CENTER CONTROL acceso*”. Titula el manual versión 2019 V1.0 build 07082019, de 114 páginas en el pdf, que se incorpora al procedimiento para completar las pruebas. El mismo día 26/04/2022 se envía copia de dicho acceso y el manual integro a la reclamada. El manual contiene los mismos aspectos que detallan los folletos aportados por la reclamada, detallando la sistemática de funcionamiento y múltiples y variadas configuraciones posibles.

El manual, lo mismo que el folleto que aporta la reclamada, informa que dispone de: sensor de activación auto activación por infrarrojos, cámara de 2 MP con doble sensor de reconocimiento facial, comunicación TCP/IP, USB, RS485, Wi-Fi, Peso: 400 gr.-Modos de identificación pin, tarjeta, reconocimiento facial y combinaciones, controladora integrada, sensor de puerta pulsador timbre y relé. Figura como opción la de incorporar una foto como cara, realizar una foto desde el software o capturar rostros desde el dispositivo de control de accesos, con objeto de verificar si el dispositivo de reconocimiento facial administrado en el software puede reconocer la cara desde la foto. La imagen del dispositivo compacto y de una única pieza del manual de usuario que aporta la reclamada en documento 4 “*face recognition terminal*” es un terminal de reconocimiento facial en el que se indica que “adopta algoritmos de aprendizaje profundo, que contribuyen a reconocer la cara más rápido y con más certeza. También soporta modos de autenticación múltiples: 1:N face match, IC card autenthication, etc. Señala que la duración del reconocimiento facial es de no más de un segundo por persona y la tasa de exactitud en el reconocimiento es de más de un 99%.

e) Modo de recogida, registro y almacenamiento de los datos de los empleados utilizados para el RF. Entorno en el que se produce la comparación de la cara del sistema y si hay un único punto para ello o varios.

Manifiesta que *“es el equipo el que hace la toma de los vectores*”, solo hay un punto y el entorno es el propio equipo

f) Tipo de tecnología empleada de almacenamiento y funcionamiento del RF, servidor, algoritmo utilizado y funciones que efectúa.

“*Se compra el software que va dentro del equipo*”.

g) En cuanto a la lectura de lo datos e identificación positiva, indiquen el modo de funcionamiento y su sincronización, puntos de lectura existentes de los datos para el cotejo de la imagen y distribución en que se hallan esos terminales de lectura. Especifiquen, si cuando se presenta la cara, ¿donde se encuentra la plantilla almacenada del empleado contra la que se coteja la imagen presentada.? (si está en el lector, en una base de datos, características de estos.

Manifiesta que "*había un solo lector a la entrada con el equipo que también es uno". El equipo lleva el programa incorporado. Los vectores están en el equipo, que es totalmente autónomo. La entidad solo ve: día, hora e identidad de la persona verificada. Nadie puede ver otra cosa*."

h) Indiquen que sucede si no reconoce la cara que se le presenta, y si almacenaría la plantilla de esa persona.

Manifiesta que no sucede nada, pues el aparato no detecta los vectores, le tiene por no fichado y no almacena nada.

i) ¿Que conexiones tiene la base de datos del ordenador con los datos del rostro que se presentan por los empleados, con los datos de empleo? Sistema de asociación del registro de la cara a la identidad de la persona. Si la base de datos se almacena en servidores, tipo de servidor y localización y titularidad.

Manifiesta que no es un ordenador como tal, sino "*un equipo todo integrado, autónomo en su funcionamiento e independiente*". "*Al equipo asignado de la ECE- el sistema solo admite uno- la única información que llega es el día, hora y nombre o identidad del empleado reconocido por el sistema."*

j) Sistema de información a cada empleado sobre recogida y tratamiento de sus datos proporcionado, conteniendo la finalidad, base legitimadora y ejercicio de derechos de datos derivados del RF, y forma de acreditar su efectiva puesta a disposición.

Manifiesta que se informó en una reunión del personal y se les ratificó de forma personal e individualizada cuando pasaron a hacerse la foto, aclarándoles las preguntas, que en su caso pudieran plantear, que fueron pocas.

k) Acreditación de que el sistema de control horario a través de la tarjeta era usado impropiamente.

Manifiesta que el uso inapropiado de tarjetas de registro del horario por algunos empleados no es fácil de acreditar siendo ese el problema que permite realizar fraudes en el registro horario sin ser detectado. Aportan documento 5, una carta de un empleado al Consejo Rector, y el orden del día de la "*asamblea personal*" de 18/02/2020 que contiene en un punto del día "*información sobre el registro de jornada de trabajo*" en el que se refiere el asunto que se trató esta cuestión por supuestamente pasar la tarjeta de otro compañero en 30/01/2020 y haber recibido una amonestación, indicando "*en relación a las aseveraciones que alguna compañera ha realizado*", niega los hechos, y manifiesta que cuando se encontraban en la fila varios compañeros esperando en orden delante de el, "*nos ha entregado su tarjeta y la hemos pasado por el lector, pero nunca sin estar presente el*".

l) Copia de hoja registro de control horario generado por algún empleado con el fin de ver los datos que se marcan, e informen, si además el sistema se usaba para otras personas, o con otros fines.

Indica que el sistema solo se usó para la finalidad de registro de horario. Acompañan una copia de un registro de un empleado anonimizado como documento número 6 apreciándose

que para esa personas, se puede agrupar los registros por días de la semana, figurando los registros horarios anotados con varias entradas y salidas en algunas jornadas.

m) Croquis de imagen de espacios en los que se sitúan los dispositivos para las tomas del rostro para el registro de la jornada, explicando si existen interrupciones de tiempo de trabajo efectivo y si se tiene que volver a registrar la cara en cada ocasión que se entre o salga o como funcionaría el régimen de pausas.

Indica que cuando sistema estaba implantado, sí que recogía las paradas o descansos pues no se necesitaba contacto con superficies a través de las manos.

Manifiesta que solo hay un dispositivo conforme al croquis que acompaña. "*Está ubicado en una mesa, en un pequeño cuarto* destinado a tal fin al que se accede desde un patio por una puerta. Se aprecia que el sistema se limitaría a presentar la cara ante el dispositivo y volver a salir por donde se ha entrado, como registro de presencia y que captaría fecha, hora y datos del empleado.

n) Valor umbral en el que el software indica que se ha producido coincidencia entre las dos imágenes faciales que se comparan, y que recomendación para este caso da el fabricante.

Indica que se desconoce, ya que "*se compró un software de un proveedor externo*."

o) Copia del registro de actividades del tratamiento: "control horario por reconocimiento facial" en documento 8, figurando como finalidad: "*control horario de empleados a través de reconocimiento facial*".

Legitimación: "contrato laboral existente con los usuarios. artículo 6. b) RGPD, obligación legal de realizar el registro de la jornada laboral de los empleados, artículo 6.c), necesidad de control de los trabajadores: artículo 6. f), cumplimiento a través del personal de las funciones de interés público encomendadas: artículo 6.e)

"Categorías de datos minucias del rostro sin salida del equipo de lectura día y hora de lectura nombre y apellidos del empleado"
Cesión de datos: no se prevén salvo en su caso administración laboral y juzgados laborales. Solo datos reportados por el equipo

Periodo de conservación mínimo cuatro años, máximo 10 años, los datos reportados por el equipo de lectura. Minucias del rostro, son eliminados al cese de la relación laboral.

Medidas de seguridad: cifrado de las minucias del rostro y conservación de los datos estanca en el equipo.

p) Bajo su punto de vista, que significado otorga a la expresión "*sistema biométricos estadísticos*" al que alude en alguno de sus escritos.

Indica que esto es información que da el fabricante sobre cómo opera el tratamiento.

Indica que el sistema solo recoge unas minucias o características especiales concretas, en general la posición o dimensiones de elementos de la huella o el rostro fundamentalmente que no permiten construir la propia huella ni el rostro de una persona. Se trata de destacar que no se guarda en el sistema la fotografía de la persona sino unas minucias especiales y con el término estadístico que son diferenciadoras solo dentro del propio grupo comparativo-los empleados de la entidad-.

q) Que intereses y derechos de los empleados, y medidas de seguridad para sus datos se han tenido en cuenta en la instauración del sistema de RF.

Manifiesta que el interés para el establecimiento ha sido la salud del personal, tomándose la medida en contexto de pandemia, confinamiento y lucha contra la COVID, pretendiendo evitar contagios derivados del uso de tarjetas de mano.
En cuanto a las medidas de seguridad se vuelve a insistir en que el aparato es estanco y autónomo por lo que no hay ninguna circulación de los datos o minucias que del rostro toma. Además, cifra los datos, por lo que éstos no se pueden utilizar por nadie, ni para nada. El aparato toma las minucias del rostro diferenciadoras, en comparación con el resto que tiene del grupo, las cifra, y las procesa, conservándolas para hacer las identificaciones y solo reporta el resultado, consistente en día, hora e identidad de la persona, sin que esas minucias circulen, ni se usen para nada, ni se puedan usar para otros fines.

r) Acuerdo por el que se aprobó la instauración del sistema de RF para el control horario.

Aporta copia de documento 9, certificado que señala que en la reunión del Consejo Rector de la Entidad de 31/03/2020, se adoptó el acuerdo de:

"*El presidente informa que, ante la expansión del virus COVID-19, y en evitación de la proliferación de contagios entre los trabajadores de esta entidad, que proceden diariamente al fichaje dentro de su jornada laboral, se tendría que determinar otro sistema de registro. Después de un largo debate al respecto, se acuerda por unanimidad, proceder a la adquisición de un sistema biométrico facial para el control de accesos, eliminando así la posibilidad de cualquier contacto físico con el sistema mencionado*"

s) Quien es el titular de las instalaciones, dominio publico urbanizado sobre el que recae la obligación de conservar de esa entidad, y si el mismo tomó parte en la decisión de uso del RF.

Indica que el titular de algunas de las instalaciones, como por ejemplo el terreno y edificaciones en que se ubican las oficinas de la propia entidad es esta misma.

Otras instalaciones como pueden ser los viales, la red de saneamiento, espacios verdes, o cualquier instalación o espacio de dominio público, son titularidad de los Ayuntamientos de ***LOCALIDAD.1y de Nuevo Baztán.

"Los Ayuntamientos no participaron en la toma de decisión, puesto que son parte del Consejo pero sin voto."

t) Qué funciones de las públicas que tiene atribuidas ejercita cuando decide el uso de dispositivos técnicos para la recogidas de datos en base a RF de los empleados para su control horario.

Manifiesta que las de conservación de las instalaciones de dominio público de la urbanización, las cuales se llevan a la práctica y se realizan a través de sus empleados de conformidad con los estatutos de la entidad.

Reiteran su consideración, ya hecha en las alegaciones de que es la persona, es decir, la entidad como ente público administrativo y no la actividad que ejerce- que la considera también pública administrativa- lo que determina la posibilidad de imponer un tipo de sanción u otro, sin que puedan realizarse interpretaciones expansivas sobre las que establece la ley y menos para imponer una sanción.

OCTAVO: Con fecha 3/05/2022 se emite propuesta de resolución del literal:

"*Que por la Directora de la Agencia Española de Protección de Datos se sancione con apercibimiento a* **ENTIDAD URBANÍSTICA COLABORADORA DE CONSERVACIÓN EUROVILLAS***, con NIF G79414033, por las infracciones del RGPD:*

-artículo 9.2.b) del RGPD, tipificada en el artículo 83.5 a) del RGPD y en el 72.1. e) de la LOPDGDD.

-artículo 35 del RGPD, tipificada en el artículo 83.4 a) del RGPD y en el 73.t) de la LOPDGDD."

Se reciben alegaciones el 17/05/2022, en las que indica:

- La propuesta no explica en que consiste la identificación unívoca que hace que los datos sean considerados especiales. Para estar ante una categoría especial de datos personales, no solo tenemos que estar ante datos biométricos, sino ante datos biométricos dirigidos a identificar de forma unívoca o única a una persona. Que no se consideren datos especiales hace que no se requiera evaluación de impacto.
unívoca

- No se ha tenido en cuenta la manifestación de que "*no utilizan imágenes de rostros, sino descripciones de estos que se traducen en ciertos patrones del dibujo del rostro*" y que el sistema solo toma "*posición o dimensiones del rostro que no permiten reconstruir el rostro de la persona, las cuales podrían coincidir en otras muchas personas por lo que no permiten la identificación inequívoca del sujeto, mas que dentro de un grupo reducido de personas como es el personal de la entidad*" "*no se guardan datos identificativos inequívocos de ningún trabajador*". "*En el procedimiento no se ha realizado un análisis o peritaje de qué capta realmente el lector*, siendo la carga de la prueba de esa Agencia, por lo que no está acreditado que lo expuesto por esta parte no sea así". "*En este sentido, se rechaza la incorporación al expediente como prueba del supuesto Manual de usuario localizado por el instructor en Internet a través de una búsqueda genérica en Google, habiendo localizado el mismo en un enlace en la dirección principal web* ******URL.1*** *(que no da ningún resultado), por desconocerse si dicho Manual es el correcto, ni haberse reclamado siquiera al fabricante o haberse confirmado con el mismo su corrección. Todos los hechos y conclusiones que se realizan en base a dicho Manual no pueden tenerse por acreditados ni darse por correctos, dado que no es una prueba obtenida con las debidas garantías de veracidad y certeza*."

-Reitera que si existía causa que levantaba la prohibición del tratamiento si se considerase el mismo dato especial. "*Las letras g) y h) del articulo 9.2 del RGPD por si solas, de forma individual y mas puestas en relación entre ellas con la propia b) justificarían el tratamiento*", dada la extraordinaria situación de pandemia vivida. "*La letra h) encaja mejor porque habilita el tratamiento cuando es necesario para fines de medicina preventiva o laboral*".

-Reitera que no es causa suficiente manifestar que antes controlaban la jornada laboral con tarjetas, dada la manipulación y fraudes que se han dado "*que han explicado y justificado*".

- "*Se rechazan las alegadas bases de legitimación, por considerarse que no está justificada la utilización de un medio que esa Agencia considera muy intrusivo, no guardando proporcionalidad, y porque, además, anteriormente, el control de la jornada laboral se hacía por medio de tarjetas sin que se hayan justificado los problemas que las mismas presentaban*". "*Existe base jurídica para ello, si bien esa Agencia lo acaba denegando en base a un principio jurídico indeterminado: "el de la proporcionalidad".* "*La proporcionalidad", no deja de ser algo subjetivo y relativo, no algo claro e indubitado. Se puede discutir sobre ello. Esta parte, puede llegar a aceptar, que si la Agencia así lo considera, no esté justificado el tratamiento en atención a ese juicio de proporcionalidad entre el interés de la Entidad y los derechos de los empleados, pero otra cosa muy distinta es imponer una sanción*."

- No responde a la situación alegada, que se presentaba en el momento de la instauración del reconocimiento facial, la de la extraordinaria y grave situación sanitaria que ponía en peligro la vida y la salud de los trabajadores. Reitera la importancia del desempeño de las funciones de los empleados cuando la gente pasaba mas tiempo que nunca en sus casas y que resultaron muchos empleados afectados, queriendo con ello evitar que tuvieran que controlar la jornada con el lector de huellas.

-Falta de culpabilidad que se desprende de la situación extraordinaria y grave del periodo en el que se instauró el sistema. Consideran que es inexistente. Además, en la resolución se indica que es la primera resolución por uso de RF en el control de jornada laboral.

HECHOS PROBADOS

1) Con fecha 12/03/2020, la reclamada informa a sus 38 empleados a través de sus representantes, que por la situación de coronavirus, va a implantar para el registro diario de jornada laboral, el sistema de reconocimiento facial (RF). El 30/04/2020 la reclamada comunica su instauración a partir de 6/05/2020. Antes de la declaración de la pandemia, en 1/03/2020, la empresa tenía implantado el sistema de huella dactilar para el control del registro horario laboral, en el trámite del cual había informado a las empleados que las tarjetas utilizadas anteriormente, eran susceptibles de traspasarse para fichar entre empleados en nombre de otros para la misma función. El cambio al RF, entre otros motivos, manifestó la reclamada, se hizo por evitar el contacto con el lector de huella por la propagación de la COVID.

2) La reclamada es una entidad urbanística colaboradora de conservación constituida con carácter obligatorio desde 1988, agrupando unos cuatro mil propietarios, en unas tres mil vi-

viendas unifamiliares, formando una población de más de diez mil habitantes, según la reclamada).

3) Los empleados de la reclamada prestan en algunos casos régimen de trabajo a turnos, o servicios de urgencias con atención de 24 horas al día, y además, tareas típicas relacionadas con el fin de las entidades de conservación urbanística: conservar la urbanización y el mantenimiento de las dotaciones e instalaciones de los servicios públicos, a título de ejemplo: realización de obras ordinarias y extraordinarias e instalaciones, labores como limpieza y vadeo de calles, obras a conservar y mantener, pueden ser de vialidad (calzada, aceras, aparcamiento y red peatonal), red de saneamiento (colectores, sumideros, depuradoras), de alcantarillado, de suministro de agua (potable, para el riego, hidrantes contra el fuego), de suministro de energía eléctrica (conducción, distribución y alumbrado público), y jardinería y arbolado en parques, jardines y vías públicas, amueblamiento y mobiliario urbano, para su uso y disfrute, titularidad pública de los Ayuntamientos de ******LOCALIDAD.1*** y de ******LOCALIDAD.2*** espacios en cuyo ámbito se localiza la reclamada.

La reclamada adoptó el 31/03/2020, el acuerdo de registrar la jornada diaria laboral para empleados de su entidad, mediante el uso de un sistema biométrico de RF, teniendo en cuenta la expansión de la COVID-19, y en evitación de la proliferación de contagios entre los trabajadores. Manifiesta en el traslado la reclamada, que el RF es "*el más adecuado para garantizar la salud de los trabajadores"*, "*efectivo y proporcional*" sin documentación que soporte dichas afirmaciones.

4) En el registro de actividades del tratamiento de la reclamada, figura: "*control horario por reconocimiento facial*" finalidad: "*control horario de empleados a través de reconocimiento facial*".

Legitimación: "contrato laboral existente con los usuarios artículo 6. b) RGPD, obligación legal de realizar el registro de la jornada laboral de los empleados (artículo 6.c), necesidad de control de los trabajadores (artículo 6. f), cumplimiento a través del personal de las funciones de interés público encomendadas: artículo 6.e)"

"Categorías de datos: minucias del rostro -sin salida del equipo de lectura-. Día y hora de lectura nombre y apellidos del empleado".

Cesión de datos: no se prevén salvo en su caso administración laboral y juzgados laborales-solo datos reportados por el equipo-.

Periodo de conservación; mínimo cuatro años, máximo 10 años, los datos reportados por el equipo de lectura. Minucias del rostro, son eliminados al cese de la relación laboral.

Medidas de seguridad: cifrado de las minucias del rostro y conservación de los datos estanca en el equipo."

5) El dispositivo que utiliza la reclamada lo adquirió el 30/03/2020, según su manual, diseñado para control presencial y acceso facial, SAFIER, modelo SF-AC3062KEMR-IP, fabricado en China " 1.600 caras, 2.500 tarjetas y 50.000 registros, TCP/IP, USB y WIFI, controladora integrada, Software Safire Control Center AC, tiempo reconocimiento , <0,5 sg., peso 400 gr, cámara 2 MP con doble sensor de reconocimiento facial, pantalla 5 LCD táctil, un coste de 375 euros. Figura como opciones, las de incorporar una foto como cara, realizar una foto des-

de el software o capturar rostros desde el dispositivo de control de accesos, con objeto de verificar si el dispositivo de reconocimiento facial administrado en el software puede reconocer la cara desde la foto. La imagen del dispositivo que aporta la reclamada es un terminal de reconocimiento facial en el que se indica que "*adopta algoritmos de aprendizaje profundo, que contribuyen a reconocer la cara más rápido y con más certeza*". También soporta modos de autenticación múltiples: 1:N face match, IC card autenthication, etc.

El dispositivo para el reconocimiento facial, está instalado en un ordenador protegido con contraseña, al que solo tiene acceso una persona, estando los datos biométricos encriptados, no siendo extraíbles. El dispositivo que lleva dentro su propio software hace la propia extracción de puntos de referencia de la cara tras hacer la fotografía y crea un patrón. El dispositivo dispone de un solo lector. Proporciona al ordenador de la reclamada informes sobre hora, fecha y empleado en cada ocasión que entra y o sale , para lo cual tiene que pasar por la habitación en la que se produce la captura de la imagen.

6) Técnicamente, de la información extraída del expediente, por comunicación de reclamada a reclamante, manifestaciones de la reclamada, y documentos aportados, el sistema de RF con fines de registro diario de jornada laboral consiste en un dispositivo colocado en una habitación frente al que los empleados presentan la cara y a través del RF, registra la hora, fecha y nombre y apellidos del empleado.

El sistema del software funciona extrayendo imágenes bidimensionales del rostro, no conserva imágenes o fotografías del rostro, sino que traduce la toma de la fotografía que la empresa les hizo presencialmente a los empleados a una plantilla, con las características de los parámetros capturados, plantilla que se guarda en el equipo o sistema vinculada con el nombre y apellidos del empleado. Cuando se captura una muestra biométrica de la persona, al entrar o salir del trabajo, la compara con las plantillas registradas y da como resultado la hora, fecha y el nombre y empleado de la persona que entra o sale del turno de jornada. En cada ocasión que el empleado ha de hacer una interrupción de la jornada, debe volver a entrar en la habitación y presentar la cara para su registro. Los datos tratados se encuentran en los servidores de la entidad. De acuerdo con la reclamada, los datos registrados se almacenen en el mismo dispositivo en el que tiene lugar el registro.

7) La reclamada no ha aportado a la AEPD la evaluación de impacto del tratamiento de datos biométricos de RF para el registro de la jornada diaria laboral de sus empleados, alegando que no trata datos biométricos de carácter especial porque no identifican de manera univoca a una persona.

8) Sobre información a los afectados de la recogida y tratamiento de sus datos, conteniendo la finalidad, base legitimadora y ejercicio de derechos derivados del tratamiento de reconocimiento facial para el registro diario de jornada laboral, manifestó la reclamada que se informó en una reunión del personal y cuando pasaron a hacerse la foto. Figura que la reclamada, en documento 6 aportado por la reclamante, el 30/04/2020, le informa de la implantación del RF: "*Este sistema funciona a partir de la identificación de un porcentaje de características extraídas del rostro, sin tomar una imagen en tres dimensiones de las caras, entendemos que esta medida es menos invasiva que la grabación del momento del fichaje por cámara, que además suponía el contacto físico con un lector de tarjeta compartido. El fin único de estos datos es el fichaje de personal y análisis de los tiempos de trabajo para el cumplimiento del decreto*

ley 8/2019, con objeto de analizar los datos en toma de decisiones y la defensa de sus intereses legítimos". "*Estos datos se encontrarán en los servidores de esta entidad, en ningún caso en la nube*". Con ocasión de la implantación del anterior sistema de huella dactilar para lo mismos fines, las partes habían intercambiado escritos sobre el uso, fines e información y constaba la disconformidad de la reclamante con el sistema.

9) Con fecha 17/09/2021, en alegaciones al acuerdo, la reclamada indicó que "*se ha vuelto al sistema de fichaje por tarjeta*" desde que recibió el acuerdo de inicio, aportando una factura de adquisición de dichos elementos.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

II

Es objeto de valoración en este procedimiento el ajuste normativo que se analiza en cuanto al sistema de RF para el registro diario de jornada laboral que la reclamada reconoce ha implantado y usado desde 6/05/2020, hasta recibir el acuerdo de inicio, con la finalidad de tratar los datos de los 38 empleados de su entidad para el registro diario de la jornada laboral, obligación impuesta en el artículo 34.9 del Texto Refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23/10 (ET).

No se trata en puridad del primer tipo de reclamación que por esta técnica tan novedosa ha tenido entrada en esta AEPD, habiendo sido ya resueltas algunas. Sin embargo, si se trata de la primera relacionada con el tratamiento de datos como entidad empleadora que decide utilizar el registro y almacenamiento de datos originados por el RF para la finalidad de registro diario de jornada laboral.

El ámbito de aplicación del RGPD extiende su protección, tal y como establece su artículo 1.2, a los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, definidos en su artículo 4.1 como "*toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*."

El derecho y la titularidad de los datos personales que cada persona reconocido en el artículo 18.4 de la Constitución Española, fue interpretado en la sentencia del Tribunal constitucional 292/2000 precisando que:

"*Este derecho fundamental a la protección de datos … atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la*

realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). "

" *el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. … El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin*. "

Como tipos específicos, los datos biométricos quedan definidos en el artículo 4.14 del RGPD:

«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;

Para considerarse datos biométricos en el sentido del RGPD, el tratamiento de datos sin procesar, como las características físicas, fisiológicas o conductuales de una persona física deben implicar una medición de dichas características. Dado que los datos biométricos son el resultado de tales mediciones, el RGPD indica en su artículo 4, apartado 14, que son 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* […]»Así pues, del concepto, no hay que perder de vista:

-La naturaleza de los datos: datos relativos a las características físicas, fisiológicas o conductuales de una persona física;

- Los medios y las formas de tratamiento: datos «*obtenidos a partir de un tratamiento técnico específico*»; lo que diferencia por ejemplo de las imágenes de una persona que figuran en un sistema de videovigilancia, que no pueden considerarse datos biométricos si no se han tratado técnicamente de una forma especifica con el fin de contribuir a la identificación única de esa persona. El considerando 51 del RGPD también se refiere a la no consideración sistemáticamente como un tratamiento de categoría especial de datos, a las fotografías, a menos que se les aplique un medio de tratamiento técnico especifico que "*permita la identificación o la autentificación unívocas de una persona física*".

- La finalidad del tratamiento: los datos se deben utilizar para la finalidad de identificar de manera unívoca a una persona física.

Los datos biométricos presentan la particularidad de ser producidos por el propio cuerpo y lo caracterizan definitivamente, son datos no sobre esa persona, sino que los datos refieren a la misma persona, en principio no modificables por voluntad del individuo, ni la persona puede ser liberada de ellos, no se pueden cambiar en caso de compromiso-pérdida o intrusión en el sistema. Además, debido a que los datos biométricos son propios de una persona y

perpetuos, el usuario utiliza los mismos datos en diferentes sistemas. Por lo tanto, un robo de identidad no solo es perpetuo en el tiempo, sino que afecta a todos los sistemas en que un usuario tenga almacenados sus datos biométricos. El titular por lo tanto, no tiene la posibilidad de utilizar un dato biométrico para el banco, y uno diferente para su sistema de salud, sino que utiliza la misma información para verificar su identidad en ambos, y frente a una vulnerabilidad se ven afectados todos ellos al mismo tiempo. Finalmente, el interesado no se entera de que su información esta siendo utilizada, pudiéndose obtener a través de objetos, rastros o cámaras de vigilancia.

También de partida, hay que destacar la nota del carácter restrictivo, pues por principio, su tratamiento está prohibido y solo pueden tratarse con carácter excepcional, en determinados supuestos que se contemplan en el RGPD, que prevé unos estrictos requisitos para posibilitar finalmente la puesta en funcionamiento de tales sistemas, debido a la afectación a los derechos y libertades fundamentales, por los riesgos que puede entrañar el contexto de su tratamiento, y que como señala el Considerando 51 del RGPD:" *Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales*."

El Considerando (52) "*Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular:*

- el tratamiento de datos personales en el ámbito de la legislación laboral,
- la legislación sobre protección social, incluidas las pensiones y
-con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. (...)"

III

La reclamada ha tratado datos de carácter personal, y específicamente datos biométricos. El concepto de tratamiento El RGPD define en su artículo 4:

"*2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos 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;

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

La definición de dato biométrico alude a "*tratamiento técnico*", sin especificar, excepto para reseñar que el propósito de dicho tratamiento debe ser identificar a una persona. Las características biométricas se someten a un tratamiento técnico mediante un proceso que se contiene en todos los tratamientos de datos biométricos: captura o registro de datos, almacenamiento o procesamiento y última fase de comparación.

Las fotografías de los empleados se capturan obteniendo una imagen, de la que se extraen las características a través del algoritmo, que forma parte del software del dispositivo de la reclamada. Estas características-vectores faciales, las llama la reclamada- son las medidas del posicionamiento y mediciones relativas de referencia (puntos nodales distancia: entre los ojos, forma de pómulos…) que recoge de cada imagen en cada individuo y el punto de partida natural para el tratamiento y reconocimiento automático de los individuos. La extracción de características es la que proporciona información para distinguir entre las caras de las diferentes personas según sus variaciones geométricas o fotométricas.

Se reduce la imagen bruta de las características biométricas, transformándose, conservándose información discriminada destacada que es esencial para el reconocimiento de la persona. Estas características extraídas se mantienen en una plantilla biométrica, que es una forma de representación matemática reducida de la característica original. La plantilla de referencia se almacena para su comparación. En la última fase, se comparará una muestra biométrica-como la cara- presentada al sensor con una plantilla previamente grabada. Las fases se avienen con la enumeración de lo que podría ser una operación de tratamiento de datos (recogida, almacenamiento, uso). El funcionamiento de la huella dactilar es similar, con matices no destacables por cuanto no varían en lo fundamental el modo de funcionamiento. La no referencia a su valoración en este procedimiento no puede ser valorada como pretende la reclamada en sus alegaciones.

En cuanto a que solo identifica a los pertenecientes al grupo de empleados, no es razón para no considerarse dato biométrico, que están dirigidos a que a las personas físicas se la identifique con los datos generados a partir de la extracción de sus características biométricas.

En cuando a la consideración de datos biométricos como datos especiales, hay que tener en cuenta que en las propuestas sobre el paquete de reforma de la Protección de Datos, que desembocó en la aprobación el RGPD, la Comisión Europea, solo añadió a la lista de datos sensibles, los datos genéticos. Fue el Parlamento Europeo quien añadió a la lista de datos sensibles, los biométricos, cuando votó la propuesta del RGPD el 14/03/2014, a pesar de que algunas autoridades nacionales sugirieron por su naturaleza especifica añadirlos a la lista de datos sensibles.

Por un lado, la definición de datos biométricos incluye que a través del tratamiento técnico especifico, "*permitan o confirmen*" "*la identificación única*" de dicha persona. Las menciones a

"*permitan*" pueden entenderse a la identificación, la de "*confirmen*" a la verificación. Por tanto, ambas, identificación o autenticación han de ser únicas, referidas a la identificación que se produzca de la persona . La identificación única por otro lado, va mas allá de que el dato sea de una persona física identificada o identificable. Dato de persona física identificada es que esa persona se la distingue o aisla de un grupo de personas. Único, puede referirse a que los datos biométricos tienen tales particularidades que pueden identificar sin ambigüedades a un individuo

Las diferencias entre los términos identificación-autenticación se refieren al modo de búsqueda en los registros almacenados y al ingreso previo del registro, según se desprende del Dictamen 3/2012, del GT 29, de 27/04/2012, sobre la evolución de las tecnologías biométricas, momento en que los datos biométricos no gozaban de la categoría de "*especiales*" que introduce el RGPD y no se aludía por tanto al termino "*dirigidos a la identificación unívoca*". El dictamen diferenciaba entre:

"*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)."

El considerando 51 señala 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. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento*".

El artículo 9.1 junto a la prohibición de tratamiento indica que lo son, los "*dirigidos a identificar de manera unívoca a una persona física*", lo que indica que los datos biométricos, por naturaleza, no son sensibles, sino dependerá del uso o contexto en que se utilicen, las técnicas empleadas para su tratamiento, y la consiguiente injerencia en el derecho a la protección de datos.

Técnicamente, la plantilla biométrica contra la que se coteja la muestra, es el producto de una medición que identifica unívoca y únicamente al individuo. Esto es lo que por ejemplo diferencia las imágenes visionadas de una videocámara que no pueden ser consideradas dato biométrico bajo la definición del artículo 9 si no son específicamente tratadas con un medio técnico para contribuir a la identificación de una persona.

Los datos biométricos de cada empleado, adquiridos en el momento de su captación se relacionan con el nombre y apellidos del empleado que los registra, para someterlos al procedimiento técnico que convierte la imagen, el formato, en muestra biométrica y el algoritmo en plantilla biométrica, almacenándose, para que con las muestras introducidas al fichar, se comparan con la serie de plantillas biométricas almacenadas en la base de datos, es decir, la comparación no se produce con una única plantilla biométrica almacenada en el

dispositivo. El reconocimiento facial no solo es capaz de validar la identidad de forma precisa, sino que tiene información única sobre personas físicas. El algoritmo del software, sobre la muestra biométrica, extrae las características biométricas, reduce y transforma en etiqueta o números esa muestra, constituyendo una representación matemática de la característica biométrica original, que es la plantilla biométrica. La plantilla se almacena para su comparación en la ultima fase en la cual con la muestra biométrica-cara-y con la plantilla previamente grabada, está identificando unívocamente al empleado, en cada ocasión que entra o sale prestando su cara al dispositivo, por lo que se considera que los datos entran dentro del ámbito de los datos especiales.

En el presente caso, desde luego, no puede hablarse de que no se trata información ligada a datos personales de una persona identificada en cada registro horario, aunque los datos se guarden en el dispositivo cifrados/encriptados. Cada vez que un empleado se sitúa frente a la cámara, permite o confirma su identificación única a través del tratamiento que lleva a cabo el reclamante con el dispositivo adquirido. La muestra presentada se compara y el sistema tiene la función de identificación con una función biométrica, identificando únicamente al empleado que dice ser y registrando sus datos. Sobre la alegación de que el sistema solo toma "*posición o dimensiones del rostro que no permiten reconstruir el rostro de la persona, las cuales podrían coincidir en otras muchas personas por lo que no permiten la identificación inequívoca del sujeto, mas que dentro de un grupo reducido de personas como es el personal de la entidad*" "*no se guardan datos identificativos inequívocos de ningún trabajador*", se debe señalar que si no permitieran la identificación inequívoca del empleado no se produciría el registro que se ha llevado a cabo, del cual la reclamada no ha dado cuenta de ninguna irregularidad en los registros llevados a cabo con su sistema, o no hubiera superado el umbral de aceptación del dispositivo y no accedería con la consiguiente falta de anotación, como sucede si no se corresponde el patrón registrado. Por lo demás, se ha detallado el funcionamiento consistente en la transformación técnica del rasgo biométrico que permite la identificación unívoca aunque sea dentro del reducido grupo de empleados.

Sobre la incorporación del manual de usuario, del que se le envió copia completa, no se puede acoger la alegación de la falta de certeza, ya que es reflejo de las especificaciones que se detallan en los folletos que la reclamante envía, sin que la reclamada haya aportado el que si considera cierto o veraz. Las especificidades señaladas en el manual coinciden con los detalles que da del sistema autónomo que utiliza como software y que constan en los folletos enviados en pruebas por la reclamada. La tecnología disponible juega un papel determinante en la identificación de la persona (considerando 26 del RGPD) y por ello se ha de mencionar y traer al caso dicho manual, aunque sea para apreciar sus características generales. Sobre la falta de peritaje que verifique que el sistema funciona como manifiesta la reclamada, no se puede discutir que inicialmente se toma una fotografía del empleado, identificando con sus datos de empleado correlacionando su plantilla, siendo cierto que es sobre la imagen procesada sobre la que se produce a través de su captura una muestra biométrica y una plantilla, no existiendo divergencias en cuanto a su consideración, que supone per se un tratamiento de datos.

IV

El artículo 7 de la Carta de Derechos Fundamentales prescribe que toda persona tiene derecho al respeto a su vida privada, y el artículo 8.1 que toda persona tiene derecho a la protección de datos de carácter personal que le conciernen. Interpretadas conjuntamente, se infiere que puede constituir una vulneración de tales derechos cualquier tratamiento de datos por parte de un tercero, en este caso la reclamada. Esta utilización de los datos de sus empleados, cuya titularidad les corresponde, podría suponer una vulneración de su derecho a la vida privada y a la protección de datos si no resultara justificada. El artículo 8.2 de la Carta de Derechos fundamentales precisa que los datos de carácter personal solo pueden ser tratados con el consentimiento del interesado o en virtud de otro fundamento legitimo previsto por Ley. Además, los artículos 7 y 8 de la carta no son absolutos, admitiendo limitaciones, siempre que estén previstas por la Ley, respeten el contenido esencial de esos derechos y con observancia del principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás (Sentencia del Tribunal de Justicia de la Unión Europea, sala cuarta, sentencia de 15 de octubre del 2013, C/291/2012.). Estos aspectos por lo demás, se reiteran en relación con los derechos fundamentales, en el art. 52.1 *in fine* de la Carta de los Derechos Fundamentales de la UE.

Se imputa a la reclamada la infracción del artículo 9.2.b) del RGPD.

El artículo 9.1 del RGPD, indica:

" *Tratamiento de categorías especiales de datos personales*"

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

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

[…]"

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

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

[…]"

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;

Pero tratándose de datos biométricos, además de levantar la prohibición sobre su tratamiento, debe contener una de las bases jurídica legitimadoras del tratamiento contenidas en el artículo 6.1 del RGPD. El derecho fundamental a la protección de los datos, previsto en el artículo 18.4 de la CE, se sustenta, por lo que hace al caso, sobre el principio esencial que el tratamiento de datos de su titular, "*solo será licito si se cumple al menos una*" de las condiciones que prevé el artículo 6.1.a) a f) del RGPD, partiendo de la base de que cualquier tratamiento de esos datos restringe derechos de su titular por el mero hecho de sufrir dicho tratamiento, momento a partir del cual cada vez va a ser identificado con este mecanismo.

La reclamada alude en su registro de tratamiento a tres bases de legitimación, que procede examinar separadamente:

- "*el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales*;" art 6.1. b) RGPD, añadiendo que también concurre la del artículo 6.1.c) del RGPD "*El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento*".

La obligación legal del registro de jornada laboral no deriva de obligaciones asumidas entre las partes sino de normativa legal contenida en el artículo 34.9 del ET, que prevé:

"*La empresa garantizará el registro diario de jornada, que deberá incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada persona trabajadora, sin perjuicio de la flexibilidad horaria que se establece en este artículo.*

Mediante negociación colectiva o acuerdo de empresa o, en su defecto, decisión del empresario previa consulta con los representantes legales de los trabajadores en la empresa, se organizará y documentará este registro de jornada.

La empresa conservará los registros a que se refiere este precepto durante cuatro años y permanecerán a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social."

Para el control mediante el registro diario de jornada laboral de cada empleado, es necesario tratar sus datos. Diferente es el análisis de la necesidad y proporcionalidad en el medio elegido, para lo cual, se podría considerar que existen sistemas alternativos.

El Grupo de Trabajo del artículo 29, GT29 (adoptado el 8/06/2017) (creado en virtud del artículo 29 de la Directiva 95/46/CE, órgano consultivo independiente europeo en materia de protección de datos y derecho a la intimidad, cuyos cometidos se describen en el artículo 30 de la Directiva95/46/CE y en el artículo 15 de la Directiva 2002/58/CE, asumidos hoy día por el Comité Europeo de Protección de Datos, CEPD), en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, indica que "*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 solo el 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 para 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".

Debe considerarse que en este caso, previamente a la instauración del RF, la entidad contaba con tarjetas para el control de jornada, si bien no parece haber analizado otras alternativas de uso para dicho fin.

- Otra base de legitimación que da la reclamada es la "*necesidad del control de los trabajadores*", 6.1 f) del RGPD, cuando el RGPD define ese artículo, como: "*el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.",* extremo que de todos modos no desarrolla ni desarrolla el balance de la prevalencias de derechos e intereses, debiéndose añadir que esta base jurídica no aplica conforme continua la redacción del citado precepto "… *al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones*.", considerando que como entidad pública realiza por delegación dichas funciones.

- Finalmente, el "*cumplimiento a través del personal de las funciones de interés público encomendadas*", artículo 6.1.e) del RGPD, que en realidad indica: "*e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*", no resultaría tampoco aplicable, ya que el artículo 8.2 de la LOPDGDD establece que el tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, cuando derive de una competencia atribuida por una norma con rango de ley.

Así pues, la única base que podría ser de aplicación sería la 6.1.c).

Sin embargo, acudiendo al levantamiento de la prohibición que prevé el tratamiento de los datos biométricos, el artículo 9.2.b) del RGPD que es el que guarda relación con el ámbito laboral, determina que:

-el tratamiento ha de ser necesario para dicho cumplimiento,

-en la medida en que así lo autoricen los Estados Miembros,

- o un Convenio Colectivo también con arreglo al derecho de los Estados miembros, que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado.

Estos son requisitos cumulativos que suponen una garantía adicional en el tratamiento de datos de su titular, que tiene en cuenta que si la consecución de los fines previstos puede realizarse sin tratamiento de datos personales, será preferible esta vía y supondrá que no es necesario llevar a cabo tratamiento alguno de datos, y subsidiariamente, que la recogida de datos sea necesaria para la finalidad establecida o pretendida y si lo fuera, que sea proporcional.

En todo caso, en estos tratamientos, se debe ser muy cauteloso en la valoración que se efectué sobre si se reúnen dichos requisitos, ya que se están tratando datos especiales. Subsidiariamente, señala la reclamada, otros literales del artículo 9.2 del RGPD, ninguno de ellos alcanza a levantar la presunción de la prohibición del tratamiento de datos biométricos, por:

- el artículo 9.2.g): "*tratamiento es necesario por razones de un interés público esencial*", pues 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. En este caso, no hay ninguna norma que prevea la declaración de interés publico esencial en el tratamiento de los datos de imágenes faciales para el registro laboral, ni las garantías que debería llevar con esa declaración.

-que el "*tratamiento es necesario para fines de medicina preventiva o laboral",* que no guarda relación alguna con la instalación del dispositivo para los registros, dentro de un contexto de pandemia en el que no se suspende el derecho de protección de datos, disponiendo la normativa de protección de datos personales y la sectorial aplicable de una regulación para dichos casos que compatibiliza y pondera los intereses y derechos en liza para el bien común.

Así, se concluye que la causa de legitimación para realizar el control horario de la jornada laboral diaria, sólo alcanza a la obligación de realizarla, pero no a realizarla utilizando datos biométricos, y su uso, sin causa de excepción para el tratamiento, como se ha acreditado, supone la infracción del artículo 9.2.b) del RGPD.

V

El incumplimiento del artículo 9.2.b) del RGPD de la reclamada, aparece descrito en el artículo 83.5.a) del RGPD, con la referencia:

"*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;"

La LOPDGDD establece en su artículo 72.1.e) de la LOPDGDD:

"*1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes*"

*"*e*) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 9 de esta ley orgánica*."

VI

El Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, del GT 29, establece que "*Independientemente de la base jurídica de dicho tratamiento, antes de su inicio se debe realizar una prueba de proporcionalidad con el fin de determinar si el tratamiento es necesario para lograr un fin legítimo, así como las medidas que deben adoptarse para garantizar que las violaciones de los derechos a la vida privada y al secreto de las comunicaciones se limiten al mínimo*

Desde que en los años 90 del pasado siglo nuestro Tribunal Constitucional adoptó el denominado "*test alemán*" en el examen del principio de proporcionalidad, es una constante en su jurisprudencia, que las medidas que afecten a derechos fundamentales, deben ser idóneas o adecuadas, necesarias y proporcionadas en sentido estricto.

El apartado 72, de las Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de video, de 29 de enero del 2020, del CEPD, indica: "*El uso de datos biométricos y, en particular, del reconocimiento facial conllevan elevados riesgos para los derechos de los interesados. Es fundamental que el recurso a dichas tecnologías tenga lugar respetando debidamente los principios de licitud, necesidad, proporcionalidad y minimización de datos tal y como establece el RGPD. Aunque la utilización de estas tecnologías se pueda percibir como particularmente eficaz, los responsables del tratamiento deben en primer lugar evaluar el impacto en los derechos y libertades fundamentales y considerar medios menos intrusivos de lograr su fin legítimo del tratamiento*. " Es decir, habría que responder la cuestión de si esta aplicación biométrica es algo que realmente es imprescindible y necesaria, o es solo "*conveniente*".

El dictamen 3/2012, sobre la evolución de las tecnologías biométricas de 27/04/2012, del GT 29, indica que: "*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 solo el 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 para 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".*

Estas valoraciones requieren exhaustividad, partiendo en este caso, no solo de la prohibición de tratamiento de estos datos, sino considerando los riesgos de usar una tecnología intrusiva, los sesgos o la probabilidad de un error en la identificación, su interoperabilidad, la suplantación de la identidad y el tipo de identidad única, permanente e invariable que se tratan, su impacto en la privacidad de las personas, las implicaciones en cuestión de derechos fundamentales de tales sistemas y las medidas de seguridad, Su uso cada vez más extendido, e interconexión tecnológica es más probable que interfiera con estos derechos fundamentales y puede dar lugar a vulneración grave de derechos.

Los responsables del tratamiento deben garantizar que la evaluación de la necesidad y la proporcionalidad considere una evaluación exhaustiva de las opciones alternativas menos intrusivas disponibles. Por consiguiente, se ha de documentar la viabilidad de otras opciones alternativas disponibles que no requieran el uso de datos especiales, comparar todas las opciones y documentar las conclusiones. Todo ello, considerando el contexto del marco en

el que se traza el tratamiento, el cumplimiento de las obligaciones a través del registro de jornada.

La necesidad implica que se requiere una evaluación combinada, basada en hechos, sobre la eficacia de la medida para el objetivo perseguido y sobre si resulta menos intrusiva en comparación con otras opciones para lograr el mismo objetivo

La necesidad no debe confundirse con utilidad del sistema. Puede que se facilite el no tener que llevar una tarjeta, es automático e instantáneo y no excesivamente costoso. Obviamente, un sistema de RF puede ser útil, pero no tiene por qué ser objetivamente necesario (siendo esto último lo que realmente debe estar presente). Como establece el dictamen 3/2012 sobre la evolución de las tecnologías biométricas- del GT 29-, debe examinarse "*si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable".* En cuanto a la fiabilidad del sistema, hay que decir que cuanto mayor sea el numero de sistemas de identificación que se basan en datos biométricos o en una plantilla obtenida a partir de datos biométricos, mayor es el riesgo de que este dato pueda acabar siendo utilizado de manera inadecuada y dando lugar a un riesgo de usurpación o suplantación de identidad.

En cuanto a la producción de estos eventos de suplantación, la reclamada aportó un ejemplo de un solo caso acontecido dos meses antes de implantar el primer medio de control dactilar del horario. Se trata de un escrito de un empleado que no acredita fehacientemente que se hubiera producido la citada suplantación en el uso de las tarjetas de acuerdo con sus manifestaciones y la falta de un procedimiento basado en acreditar los hechos, que no es aportado. La alegación de que no se considera proporcional el uso del reconocimiento facial porque previamente utilizó el sistema de tarjeta, no es mencionada en la propuesta. De todos modos se puede concluir que no se acreditan tales usos fraudulentos por la mención de un caso, que como queda acreditado son unas declaraciones del empleado. Aparte, se podría establecer un régimen sancionador interno que disuada y sea efectivo por el uso fraudulento si fuera el caso de las tarjetas, no se justifica que el tratamiento a través del RF sea necesario para el cumplimiento de las obligaciones en materia laboral como lo es el registro de jornada laboral diaria establecido por Ley. Mencionar de todos modos que se ha vuelto tras el acuerdo de inicio a ese sistema y se han de analizar las opciones y alternativas antes de instaurar un sistema nuevo que supone una exagerada limitación del derecho de cada empleado, cuando pueden existir medios menos invasivos de la intimidad, y no optar por lo practico y cómodo cuando están en juego derechos de sus titulares. También se deben considerar los riesgos del tratamiento, que denotan una falta de consolidación plena de la confianza en el sistema, dados los pros y los contras, siendo conocedores que los sistemas biométricos pueden ser burlados y ser comprometidos sus datos e información, en formas relativamente fáciles. En este caso, el tipo de actividad, común a muchas empresas, como es el registro de jornada, no puede dar pie al tratamiento de datos especiales en bloque de colectivos, que no generan mas ventajas o beneficios para el interés general que perjuicios sobre los bienes o valores en conflicto. Se reitera que dada la finalidad que se pretende conseguir y los bienes jurídicos en liza, el contexto en el que se produce, el tipo de actividad que desarrolla el reclamante, que no entraña un riesgo importante a proteger o un bien jurídico supremo o prevalente, supone que el tratamiento especializado que plantea no puede ceder para el registro de jornada, incidiendo en el juicio de proporcionalidad, tal como reseña el Dictamen 3/12 sobre la evolución de las tecnologías biométricas.

VII

Además, el sistema de responsabilidad proactiva implantado por el RGPD, enfocado a la gestión continua de los riesgos potenciales asociados al tratamiento, impone a los responsables del tratamiento que analicen que datos tratan, con que finalidades y que tipo de tratamientos llevan a cabo, relacionando los potenciales riesgos a que están expuestos y a partir de ahí, decidir que medidas toman y aplican para asegurar su cumplimiento en función de los riesgos detectados y asumidos.

El tratamiento de RF presenta altos riesgos para los derechos y libertades fundamentales y antes de implantar un proyecto de tratamiento de datos, siempre y cuando sea probable que el mismo suponga un riesgo significativo para los derechos y libertades de las personas, como es este caso, es preciso auditar su funcionamiento, no de forma aislada sino en el marco del tratamiento concreto en que se va a emplear. La evaluación de impacto en la protección de datos personales, EIPD, es la herramienta que en el RGPD se ocupa de la garantía de cumplimiento de esta vertiente del tratamiento.

En este caso, se han de analizar los riesgos diversos que se pueden dar, incluyendo su tecnología, en el marco de un uso cada vez más intensivo de este tipo de datos. Su uso, interoperabilidad e interconexión tecnológica, es más que probable que interfiera con estos derechos fundamentales y puede dar lugar a cuestionamientos sobre su implantación.

El RGPD establece la obligación de gestionar el riesgo que para los derechos y libertades de las personas supone un tratamiento. Este riesgo surge tanto por la propia existencia del tratamiento, como por las dimensiones técnicas y organizativas del mismo. El riesgo surge por los fines del tratamiento y su naturaleza, y también por su alcance y el contexto en el que se desenvuelve.

La utilización de datos biométricos y, en particular, el RF entraña mayores riesgos para los derechos de los interesados. Es fundamental que el recurso a esas tecnologías se haga respetando debidamente los principios de legalidad, necesidad, proporcionalidad y minimización de los datos establecidos en el RGPD. Si bien el uso de estas tecnologías puede percibirse como particularmente eficaz, los responsables deben, en primer lugar, evaluar el impacto en los derechos y libertades fundamentales y considerar medios menos intrusivos para lograr su objetivo legítimo del tratamiento.

La "*aproximación basada en el riesgo"* se desarrolla en el "*Statement on the role of a risk-based approach in data protection legal frameworks WP218*" del GT 29, WP218, y no es un concepto novedoso en el marco de la protección de datos.

La gestión del riesgo para los derechos y libertades, tiene por objetivo el estudio del impacto y la probabilidad de causar daño a las personas, a nivel individual o social, como consecuencia de un tratamiento de datos personales. Por el contrario, la gestión de riesgo de cumplimiento normativo tiene por objetivo facilitar al responsable una herramienta para verificar el grado de cumplimiento de las obligaciones y preceptos exigidos legalmente con relación a una actividad de tratamiento. Por lo tanto, previamente al proceso de gestión de riesgos y como condición sine qua non para emprender una actividad de tratamiento, es preciso sistematizar la verificación de cumplimiento normativo a lo largo de todo el ciclo de vida del tratamiento. La complejidad del proceso de gestión de riesgo ha de ajustarse, no al tamaño de la entidad, la disponibilidad de recursos, la especialidad o sector de la misma,

sino al posible impacto de la actividad de tratamiento sobre los interesados y a la propia dificultad del tratamiento.

El artículo 35 del RGPD cuya infracción se imputa a la reclamada, establece la obligación de disponer de una Evaluación de Impacto en la Protección de los Datos Personales (EIPD), señalando:

"*1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.*

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del

tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento."

En desarrollo del párrafo 4, la Directora de la AEPD aprobó un listado no exhaustivo, orientativo de los tipos de tratamiento que requieren una evaluación de impacto relativa a la protección de datos, indicándose: *"En el momento de analizar tratamientos de datos será necesario realizar una EIPD en la mayoría de los casos en los que dicho tratamiento cumpla con dos o más criterios de la lista expuesta a continuación, salvo que el tratamiento se encuentre en la lista de tratamientos que no requieren EIPD a la que se refiere en artículo 35.5 del RGPD*. La lista se basa en los criterios establecidos por las "*DIRECTRICES SOBRE LA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD) Y PARA DETERMINAR SI EL TRATAMIENTO «ENTRAÑA PROBABLEMENTE UN ALTO RIESGO» A EFECTOS DEL RGPD*", revisadas por última vez y adoptadas el 4/10/2017, WP 248 rev.01 del GT 29 que los complementa y debe entenderse como una lista no exhaustiva:

"*4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD… o deducir información sobre las personas relacionada con categorías especiales de datos.*

5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física."

9*. Tratamientos de datos de sujetos vulnerables*…"

En las mismas Directrices, se señala:

"*Con el fin de ofrecer un conjunto más concreto de operaciones de tratamiento que requieran una EIPD debido a su inherente alto riesgo, teniendo en cuenta los elementos particulares del artículo 35, apartado 1, y del artículo 35, apartado 3, letras a) a c), la lista que debe adoptarse a nivel nacional en virtud del artículo 35, apartado 4, y los considerandos 71, 75 y 91, y otras referencias del RGPD a operaciones de tratamiento que «probablemente entrañen un alto riesgo», se deben considerar los nueve criterios siguientes*:

"*7. Datos relativos a interesados vulnerables (considerando 75): El tratamiento de este tipo de datos representa un criterio debido al aumento del desequilibrio de poder entre los interesados y el responsable del tratamiento, lo cual implica que las personas pueden ser incapaces de autorizar o denegar el tratamiento de sus datos, o de ejercer sus derechos. Entre los interesados vulnerables puede incluirse a niños (se considera que no son capaces de denegar o autorizar consciente y responsablemente el tratamiento de sus datos), empleados"*

La EIPD es un paso necesario para el tratamiento de datos, no siendo como se ha descrito, el único exigible, es un presupuesto al que se debe añadir el resto de los requisitos legales para el tratamiento, base legitimadora y respeto de los principios fundamentales del tratamiento de datos previsto en el artículo 5 del RGPD.

Antes de implantar un sistema de RF, el responsable debe de valorar si hay otro sistema menos intrusivo con el que se obtenga idéntica finalidad.

El tratamiento biométrico presenta, entre otros los siguientes riesgos, algunos de los cuales se contemplan en el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del GT 29 de 27/04/2012:

-La definición del tamaño (cantidad de información) de la plantilla biométrica es una cuestión crucial. Por una parte, el tamaño de la plantilla debe ser lo bastante grande para gestionar la seguridad (evitando solapamientos entre los diferentes datos biométricos, o sustituciones de identidad), y por otra, no deberá ser demasiado grande a fin de evitar los riesgos de reconstrucción de los datos biométricos

-Riesgos que conlleva la utilización de datos biométricos para fines de identificación en grandes bases de datos centralizadas, dadas las consecuencias potencialmente perjudiciales parar las personas afectadas.

-No hace falta decir que toda pérdida de las cualidades de integridad, confidencialidad y disponibilidad con respecto a las bases de datos sería claramente perjudicial para cualquier aplicación futura basada en la información contenida en dichas bases de datos, y causaría

asimismo un daño irreparable a los interesados. Por ejemplo, si los datos registrados de una persona autorizada se asociaran con la identidad de una persona no autorizada, esta última podría acceder a los servicios de que dispone el propietario del dato, sin tener derecho a ello. El resultado sería un robo de identidad, que (independientemente de su detección) quitaría fiabilidad al sistema para futuras aplicaciones y, en consecuencia, limitaría su libertad.

- La transferencia de la información contenida en la base de datos.

-Se puede crear la ilusión de que la identificación a través de la cara siempre es correcta, por ello se debe incluir un análisis de los errores que se pueden producir en su uso, medidores de evaluación del rendimiento, tasa de falsa aceptación- probabilidad de que un sistema biométrico identifique incorrectamente a un individuo o no rechace a un individuo que no pertenece al grupo, y tasa de falso rechazo o falso negativo: no se establece la correspondencia entre una persona y su propia plantilla. Frente a las decisiones que afecten jurídicamente a una persona, toda decisión que se adopte en base a ello, como podría ser en sistemas de registro y control horario, la deducción de retribuciones por registro con el sistema, que solo debería efectuarse salvaguardando los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

-Vinculación: un gran número de servicios en línea permiten a los usuarios cargar una imagen para vincularla con el perfil del usuario. El RF 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. Este impacto aumenta con el creciente despliegue de estas tecnologías. Cada individuo puede figurar en uno o varios sistemas biométricos.

-Deben adoptarse medidas de seguridad con motivo del tratamiento de datos biométricos (almacenamiento, transmisión, extracción de características y comparación, etc.) y sobre todo si el responsable del tratamiento transmite esos datos a través de Internet. Las medidas de seguridad podrían incluir, por ejemplo, la codificación de las plantillas y la protección de las claves de codificación aparte del control del acceso y una protección que convierta en virtualmente imposible la reconstrucción de los datos originales a partir de las plantillas. Adicionalmente, uso de máscaras realistas o de uso de fotos para intentar engañar al sistema, siempre en conexión con los avances y el estado de la técnica., teniendo en cuenta que los sistemas biométricos más eficaces a la hora de reconocer a una persona son también los más potencialmente vulnerables

En cuanto a las garantías a implementar que se han de contener en la EIPD, la Guía "*La protección de datos en las relaciones laborales*" de la AEPD contempla, a título de referencia diez aspectos que se pueden tener en cuenta.

Asimismo, el documento de trabajo sobre biometría, adoptado el 1/08/2003 del GT29, opina que los sistemas biométricos relativos a características físicas que no dejan rastro (por ejemplo la forma de la mano, pero no las huellas digitales) o los sistemas biométricos

relativos a características físicas que dejan rastro pero no dependen de la memorización de los datos poseídos por una persona distinta del interesado (en otras palabras, los datos no se memorizan en el dispositivo de control de acceso ni en una base de datos central) crean menos riesgos para la protección de los derechos y libertades fundamentales de las personas (Se pueden distinguir los datos biométricos que se tratan de manera centralizada de los datos de referencia biométricos que se almacenan en un dispositivo móvil y el proceso de conformidad se realiza en la tarjeta y no en el sensor o cuando éste forma parte del dispositivo móvil).

-Se acepta generalmente que el riesgo de reutilización de datos biométricos obtenidos a partir de rastros físicos dejados por personas sin darse cuenta (por ejemplo: huellas digitales) para fines incompatibles es relativamente bajo si los datos no están almacenados en bases de datos centralizadas, sino en poder de la persona y son inaccesibles para terceros. El almacenamiento centralizado de datos biométricos incrementa asimismo el riesgo del uso de datos biométricos como llave para interconectar distintas bases de datos, lo cual podría permitir obtener perfiles detallados de los hábitos de una persona tanto a nivel público como privado. Además, la cuestión de la compatibilidad de los fines nos lleva a la interoperabilidad de diferentes sistemas que utilizan la biometría. La normalización que requiere la interoperabilidad puede dar lugar a una mayor interconexión entre bases de datos.

La reclamada no contempla diversos y variados elementos y escenarios que se han señalado en este apartado en su valoración de riesgos, y ha manifestado que no trata datos de carácter especial. Sin embargo, los datos si que son de dicho tipo, por cuando identifican ineludiblemente al empleado, ya que tiene su plantilla guardada y cuando presente la muestra, la comprueba de entre todas las existentes, identificando plenamente a su titular a través de las muestras que se guardan en el dispositivo. Como ya se señalado previamente se produce un tratamiento de este tipo de datos.

De conformidad con las evidencias de las que se dispone, se considera que los hechos expuestos incumplen lo establecido en el artículo 35 del RGPD, con ausencia de cualquier tipo de análisis documentado del impacto vinculado al tratamiento de reconocimiento facial del que deriven la adopción de medidas y garantías específicas.

VIII

Sobre la inexistencia de culpabilidad porque actuó con animo de proteger la salud de su personal, intentando garantizar la prestación de sus servicios esenciales durante el período extraordinario de confinamiento, y que es la primera resolución por uso de RF en el control de jornada laboral, se ha de indicar que por culpabilidad debe entenderse el juicio personal de reprochabilidad dirigido al autor de un hecho típico y antijurídico. Ello implica que el autor sea causa de la acción que supone la conducta ilícita. que sea imputable sin que concurran circunstancias que alteren su capacidad de obrar y que sea culpable, esto es que haya actuado con conciencia y voluntariedad bien a título intencional bien a título culposo.

Cabe indicar que el principio de culpabilidad impide la admisión en el derecho administrativo sancionador de la responsabilidad objetiva, también es cierto, que la ausencia de intencionalidad resulta secundaria ya que este tipo de infracciones normalmente se cometen

por una actuación culposa o negligente, lo que es suficiente para integrar el elemento subjetivo de la culpa. El campo de la simple inobservancia es el clásico de la imprudencia o negligencia, en sus distintos grados. Desde el punto de vista material, la culpabilidad consiste en la capacidad que tiene el sujeto obligado para obrar de modo distinto y, por tanto, de acuerdo con el ordenamiento jurídico, dentro de lo que es una interpretación jurídica razonable. Por tanto, lo relevante es la diligencia desplegada en la acción por el sujeto, y la lo que excluye la imposición de una sanción, únicamente en base al mero resultado, es decir al principio de responsabilidad objetiva. En este sentido el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, cuando el infractor no se comporta con la diligencia exigible.

"No obstante, el modo de atribución de responsabilidad a las personas jurídicas no se corresponde con las formas de culpabilidad dolosas o imprudentes que son imputables a la conducta humana. De modo que, en el caso de infracciones cometidas por personas jurídicas, aunque haya de concurrir el elemento de la culpabilidad, éste se aplica necesariamente de forma distinta a como se hace respecto de las personas físicas. Según la S.TC. 246/1991: "(...) esta construcción distinta de la imputabilidad de la autoría de la infracción a la persona jurídica nace de la propia naturaleza de ficción jurídica a la que responden estos sujetos. Falta en ellos el elemento volitivo en sentido estricto, pero no la capacidad de infringir las normas a las que están sometidos. Capacidad de infracción y, por ende, reprochabilidad directa que deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona jurídica que está sujeta al cumplimiento de dicha norma ". En esta misma línea, se pronuncia la S.TS. de 24 de noviembre de 2011 -recurso nº. 258/2009-. "(Sentencia 1456/2021 del Tribunal Supremo, sala tercera, de lo contencioso administrativo, sección tercera, de 13/12/2021, recurso 6109/2020.

Sobre la concurrencia de la pandemia ya se ha explicado su interacción en el tratamiento de datos y su conjugación con los derechos de los titulares. El desempeño de servicios esenciales no implica el uso del sistema de reconocimiento facial que partiendo de su prohibición precisa de un análisis de su impacto y las garantías de los derechos de sus titulares. Sobre que es un caso novedoso, se han citado en esta resolución dictámenes y directrices del GT 29 que suponen interpretación de la norma, publicadas en la web, que se remontan a: 2003, 2012, 2017, 2018 y 2020. Junto a ello, también existen informes de la materia de la AEPD publicados en la web, elementos que contribuyen a una razonable y cautelosa interpretación de la clara prohibición de tratamiento de datos en la norma, en un sistema de valoración de riesgos y proactivo, que no consta llevara a cabo la reclamada. Por tanto, se desprende que si existe culpabilidad por parte de la reclamada cuando podría haber actuado de forma distinta a la que lo hizo, sin la exigencia de una diligencia exagerada.

IX

El artículo 83.4 RGPD señala: *"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*

a) Las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a

39, 42 y 43;"

La LOPDGDD establece en su artículo 73.t):

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible."

X

El artículo 83.7 del RGPD señala que "*Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro*."

En tal sentido, señala el artículo 77 de la LOPDGDD:

"*1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:*

[…]"

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas"

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica.

El artículo 26.1 del RGU, señala que: "*las entidades urbanísticas colaboradoras tendrán carácter administrativo y dependerán en este orden de la administración urbanística actuante*".

La reclamada es una entidad que ostenta carácter jurídico-administrativo para el cumplimiento de sus fines, constituida en este caso con carácter obligatorio por voluntad de sus miembros, según se refleja en los Estatutos, que tiene por objeto la conservación de las obras de urbanización y mantenimiento de las dotaciones y servicios por parte de sus propietarios agrupados

La Ley 29/2001 de 1707, del suelo, de la Comunidad de Madrid (BOCM de 27/07/2001, que dispone de competencia exclusiva en materia de Urbanismo en su artículo 137 indica: *"Entidades urbanísticas de conservación":*

"1*. Las entidades urbanísticas de conservación son entidades de Derecho público, de adscripción obligatoria y personalidad y capacidad jurídicas propias para el cumplimiento de sus fines.*

2. Se rigen por sus estatutos en el marco de la presente Ley y sus normas reglamentarias y adquieren personalidad jurídica desde su inscripción en el registro administrativo correspondiente de la Consejería competente en materia de ordenación urbanística."

El objetivo por el que se constituye una entidad urbanística de conservación es atribuir a los propietarios de una determinada urbanización la conservación de esta, función que inicialmente le correspondería al Ayuntamiento o Ayuntamientos de los términos municipales en los que se encuadra la urbanización. Estas entidades reciben tanto aportaciones de los propietarios que pagan la correspondiente cuota como fondos públicos. Dada esta naturaleza pública calificada de entidad de Derecho Público, dependiente de la Consejería de Medio Ambiente, Vivienda y Agricultura, le resultaría de aplicación el régimen establecido en el artículo 77 de la LOPDGDD en cuanto a la imposición de sanción de apercibimiento.

Por tanto, no procedería imposición de sanción de multa administrativa.

la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: SANCIONAR con apercibimiento a **ENTIDAD URBANÍSTICA COLABORADORA DE CONSERVACIÓN EUROVILLAS**, con NIF G79414033, por las infracciones del RGPD:

-artículo 9.2.b) del RGPD, tipificada en el artículo 83.5 a) del RGPD y en el 72.1. e) de la LOPDGDD.

-artículo 35 del RGPD, tipificada en el artículo 83.4 a) del RGPD y en el 73.t) de la LOPDGDD.

SEGUNDO: NOTIFICAR la presente resolución a **ENTIDAD URBANÍSTICA COLABORADORA DE CONSERVACIÓN EUROVILLAS**, con el envío de ANEXO GENERAL y a la **CONSEJERÍA MEDIO AMBIENTE, VIVIENDA Y AGRICULTURA de la CCAA de MADRID.**

TERCERO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

CUARTO: De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-050522

Mar España Martí

Directora de la Agencia Española de Protección de Datos

ANEXO GENERAL

Reclamante: A.A.A.