

- **Procedimiento N°: PS/00010/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: A.A.A. (en adelante, la reclamante) con fecha 25/11/2019 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra **DAVISER SERVICIOS, S.L.** con NIF **B43586809** (en adelante, el reclamado). Los motivos en que basa la reclamación son:

“La empresa tiene instalado un fichero en la puerta de acceso en la entrada de la nave industrial con lectura de huella digital y clave de operario”.

“La empresa tiene instalados también cuatro ficheros más en las puertas de acceso al vestuario, a lavabos y comedor también con lectura de huella digital y clave de operario”.

Manifiesta:

-El lector de huella de los lavabos falla muy a menudo ya que tienen las manos sucias por las condiciones de trabajo motivado por los guantes que utilizan y la suciedad del lector se va acumulando. Al lavabo para lavarse las manos se accede después de fichar.

-Prestan sus servicios tanto empleados de la plantilla y de ETT de dos empresas más.

-También se toman imágenes con el sistema de videovigilancia que enfoca a la puerta del lavabo.

Aporta:

-Copia de informe de inspección de Trabajo y Seguridad Social de 14/12/2018, en el centro de trabajo del reclamado, con objeto de comprobar la utilidad de marcadores digitales y cámaras de videovigilancia. En hechos probados figura:

- El 13/11/2018 una empleada no pudo acceder a los servicios durante su jornada porque no funcionó el marcador de huella digital que franquea el acceso al mismo. *“En presencia del inspector se requiere a una empleada que acceda a los servicios y la trabajadora se ve obligada a repetir la operación varias veces para conseguir la apertura de la puerta.”*
- *“en cuanto a la instalación de los marcadores digitales y de las cámaras de vigilancia, no consta una comunicación formal a la representación legal de los trabajadores por cuanto se produjo con carácter previo a las primeras elecciones para representantes de los trabajadores en la empresa que se celebraron en septiembre de 2017.”*

El Inspector acordó iniciar procedimiento sancionador mediante acta de infracción por ocasionar a una empleada una situación que atentó contra su dignidad y se requiere a la

empresa una modificación del sistema de acceso a los servicios a fin de evitar incidentes similares.

Manifiesta la reclamante que la empresa emitió una propuesta de negociación conjunta en junio del 2019, en donde se indicaba acerca del requerimiento de la Inspección de trabajo: *“se procederá a cambiar los pulsadores de acceso, y además, se procederá a la instalación de dos pulsadores, uno externo y otro interno para abrir la puerta en caso de emergencia”*, que finalizó *“sin conformidad alguna”*, tomando la empresa esa decisión unilateral de colocar dos pulsadores extras.

Considera la reclamante que la implantación del sistema de huella no es idónea, proporcional, ni equilibrada y que no se informó previamente de la finalidad y usos, así como del ejercicio de derechos.

SEGUNDO: A la vista de los hechos denunciados en la reclamación y de los documentos aportados por el reclamante, la Subdirección General de Inspección de Datos traslada el 3 y 17/02/2020 la reclamación al reclamado.

Con fecha 26/03/2020, el reclamado manifestó:

1) La empresa MPH le presta el *“servicio integral de gestión de horarios”*, parametrización y soporte técnico. Indica que la identificación biométrica a través de la huella dactilar consiste en el tratamiento única y exclusivamente de una serie de coordenadas relevantes obtenidas de las huellas dactilares de los usuarios que son procesadas y cifradas mediante un algoritmo, obteniéndose como resultado un código de hash conocido como *“minucia”*, garantizando su irreversibilidad.

“La información descrita, así como la obtenida del tratamiento resultante queda debidamente registrada y guardada en los servidores MPH instalados en su sede central de Las Palmas de Gran Canaria, lo que en ningún caso permitirá por parte del usuario o interesado solicitante, manipulación o variación de datos registrados.”

Indica que: *“tal como establece el Real Decreto Legislativo 2/2015 de 23/10 que aprueba el texto refundido de la ley del Estatuto de los trabajadores, (ET) en su modificación por el Real Decreto ley 8/2019 de 8/03 marzo, MPH en su calidad de encargado de tratamiento, conservará los datos generados con motivo de la prestación del servicio integral de gestión de horarios durante 4 años.”*

2) En el año 2014, se instaló el primer sistema de control de presencia solamente para los accesos de entrada y salida de la nave.

“La finalidad de estos marcadores era el control de presencia y la seguridad en el acceso a las instalaciones.”

“Sobre los nuevos marcadores de acceso a las instalaciones y a los servicios, en el año 2017 se instala un nuevo sistema de marcadores, el actual y vigente, con nuevos marcadores tanto para la entrada de salida de la nave como para el acceso a los servicios, implantando un nuevo software de tratamiento de datos en la nube.”

“La finalidad de los marcadores es el control de presencia, la seguridad en el control de acceso a las instalaciones de la empresa, y conocer el número de personas que están en el recinto de la nave”.

3) Manifiesta que la implantación del sistema de fichajes no ha tenido como finalidad controlar el tiempo que una persona está en el lavabo, *“no se guarda el tiempo de estancia en esas dependencias”*, sino que *“la finalidad es que accedan a las instalaciones “privadas de la empresa: servicio, el vestuario etcétera, sólo el personal autorizado para impedir el acceso a personal ajeno, como transportistas comerciales etcétera.”*

4) *“La decisión adoptada tras la reclamación, es el mantenimiento del sistema de fichaje.*

-Aporta tres fotografías bajo el título *“informe fotográfico de los pulsadores manuales”*. En la primera, se ve un marcador digital (fichador) y un pulsador de color negro. En el pie de la foto pone *“marcador digital de acceso a las instalaciones y pulsador de emergencia para entrar “*.

En la segunda foto, otro marcador digital y cerca un pulsador rojo situado a su izquierda sobre unos azulejos. En la tercera foto, otro marcador digital con el pulsador negro a su derecha sobre el mismo tipo de azulejos que la foto segunda, añadiendo el rótulo de estas dos últimas: *“marcadores digitales de salida de a los servicios y pulsadores de emergencia para salir”*.

-Aporta copia de contrato de encargo de tratamiento con la empresa MPH, indicando en la cláusula segunda que se pondrá a disposición del encargado del tratamiento los datos personales de nombre y apellidos, documento nacional de identidad, minucia de la huella, datos relativos al puesto de trabajo, departamento, categoría, turno, etcétera, email del usuario, firma/ firma digital y en su caso el código del trabajador que tuviera asignado, en caso contrario MPH asignará un código alfanumérico que identificará a cada usuario. Se indica que la entidad está certificado certificada en el Esquema Nacional de Seguridad y en la ISO 27001

La recogida del dato biométrico se realiza en las instalaciones del responsable del tratamiento y se llevará a cabo a través de los dispositivos hardware propiedad del encargado de tratamiento, quién mediante acceso remoto los incorpora a sus sistemas de información ubicados en las instalaciones centrales del encargado del tratamiento.

- Aporta copia del registro de actividad del encargado de tratamiento, *descripción de tratamiento de datos, indicando que presta servicios de control horario mediante terminales de fichar que transmiten a sus servidores centrales toda la información para ser tratada ya que el cliente accede a través del portal web mediante usuario y clave.*

Tipos de datos gestionados en el tratamiento de datos, DNI, nombre y apellidos código usuario/ empleado detalles del empleo, número de días de ausencia inclusive por IT a los fines del control horario/ tiempo de presencia huella otros datos biométricos este último posee la categoría especial”.

TERCERO: La Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante el 9/06/2020.

CUARTO: En el marco de las actuaciones previas practicadas por la Subdirección General de Inspección de Datos, con objeto de aclarar la respuesta del reclamado, con fecha 17/06/2020, se le solicitó:

1. Evaluación de impacto.

Respondió que no han formalizado la evaluación de impacto sobre la implantación del sistema de fichaje, dado que el *“encargado del tratamiento efectúa un tratamiento consistente en una serie de coordenadas relevantes obtenidas de las huellas, no utiliza la huella íntegramente, sino que las procesa y cifra mediante algoritmo obteniéndose la “minucia”, de modo que no se puede conocer ni establecer la huella dactilar de la persona ni tampoco conocer a quién pertenece.”*

2. Número de trabajadores de la entidad donde se ha instalado el sistema de control mediante huella dactilar. Número de personas externas que acuden a las instalaciones.

Manifiesta que se usa en la actualidad en una plantilla formada por una media de 30 personas.

“No existe un control numérico de las personas externas ajenas a la empresa que acceden, porque se trata de transportistas que acuden por tareas de carga y descarga, así como auditores de calidad de terceras empresas para controlar el producto manipulado por la empresa.”

Se podría cifrar una media de 4 o 5 visitas al día, entre transportistas cuyo acceso es diario y auditores cuyo acceso es muy irregular.”

3. Información facilitada de la existencia de una zona videovigilada mediante fotografías del cartel o carteles informativos en las que sea posible apreciar tanto su ubicación como los datos mostrados.

Adjunta fotografías en las que se aprecia dónde está colocada cada una de las 4 cámaras en la nave (una de ellas, manifiesta que no funciona, la 1) y las identifica con números. En la foto 1 se ve la cámara 1 a la derecha, que se sitúa sobre un cartel amarillo de aviso de videovigilancia y la cámara dos a la izquierda. Se ven 3 puertas azules, la de la derecha abierta que da acceso a otro espacio de la nave y las dos de la izquierda, más cercanas entre sí, cerradas, y sobre ellas existe un reloj en la pared. En estas dos puertas más cercanas entre sí, en la de la izquierda hay un símbolo de una pegatina, de aseo, o servicio.

La cámara 1 y enfoca en lateral se aprecia que debajo de la cámara dos hay dos puertas azules cercanas y sobre ellas un reloj en la pared en la puerta en la puerta.

La foto 2 es una vista más amplia de estas tres puertas, pero se ve una puerta más que no se veía en la foto 1. Esta puerta adicional (puerta cuatro) se encuentra abierta, se halla a la izquierda de la que tiene el símbolo de pegatina de aseo. Tras ella está otra puerta cerrada (puerta cinco). En la antesala de la puerta cinco, se ve un fichador que tiene a su derecha un pulsador de acceso. Este fichador se corresponde con la tercera foto del *“informe fotográfico de los pulsadores manuales”*, que reza como *“marcadores digitales de salida de los servicios y pulsadores de emergencia para salida de a los servicios y pulsadores de emergencia para salir”* que la reclamada aportó en la respuesta de 26/03/2020 en fase de traslado de la reclamación

En la puerta con la pegatina de aseo, a su izquierda figura también un fichador y un pulsador de acceso en su parte superior izquierda. Este fichador se corresponde con la primera foto del informe fotográfico de los pulsadores manuales, *“marcador digital de acceso a las instalaciones y pulsador de emergencia para entrar”* que la reclamada aportó en la respuesta de 26/03/2020 en fase de traslado de la reclamación.

En todas las puertas en el suelo está marcado con franjas amarillas y negras

Aporta imágenes que capta el monitor en el que se proyecta la visión de cada cámara, solo se ven tres imágenes. (cámara 2, 3 y 4).

Se ve en el monitor la imagen identificada como CÁMARA 2, obtenida por la cámara que se sitúa sobre un cartel amarillo informativo de videovigilancia. El reclamado la identifica como CÁMARA 1, que señala “no funciona”, si bien si se ven las imágenes en el citado monitor. Se puede ver todo lo largo de la zona lateral de la nave, incidentalmente, al inicio se halla lo que puede ser la zona del acceso a lavabos, el suelo tiene franjas amarillas y negras. Teniendo las puertas un fichador, se puede identificar a cualquier persona que a ellos acceda o salga.

Cercana a la puerta del acceso al lavabo y sobre ella, se halla otra cámara que manifiesta que enfoca hacia la zona de entrada de camiones.

Manifiesta que “Las cámaras 3 y 4 enfocan directamente al almacén y están mal ubicadas, de manera que si el almacén se encuentra lleno de contenedores- como pasa actualmente - no se visiona ninguna panorámica del almacén.”

4. Explicar las causas que han motivado la instalación de las citadas cámaras y cuál es la finalidad de su instalación.

Las causas de la instalación de las cámaras son el control del stock del almacén y zona de producción, cámaras 1, 3 y 4, y la visión de la entrada de camiones a la nave, cámara 2.

5. Facilitar copia de las comunicaciones remitidas a los empleados y sus representantes para informar de la finalidad de la instalación de las cámaras de videovigilancia.

Manifiesta que los trabajadores han “declinado firmar el documento sobre confidencialidad y tratamiento de datos”. El documento que aporta, es un acuerdo de confidencialidad por acceder el usuario a datos (en sus funciones indica que tiene acceso a sistemas y soportes en los que se contienen información relativa a datos de carácter personal). Su cláusula octava indica que trata sus datos por la gestión de la relación laboral. No se contiene nada sobre el sistema de uso de cámaras. Tampoco en anexo 4, que es un compendio de la normativa de protección de datos.

6. Indicar el plazo de conservación de las imágenes registradas, junto con el detalle de las medidas adoptadas para garantizar que sólo el personal autorizado accede a las grabaciones.

Manifiesta que las imágenes no se conservan, sólo pueden visionarse en directo y el acceso al monitor se realiza sólo por el Administrador y Gerente de la empresa.

QUINTO: Con fecha 19/02/2021, la Directora de la AEPD acordó:

“INICIAR PROCEDIMIENTO SANCIONADOR a DAVISER SERVICIOS, S.L., con NIF B43586809, por la presunta infracción del artículo 5.1.c) del RGPD conforme a lo establecido en el artículo 83.5. a) del RGPD.

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, la sanción que pudiera corresponder sería de apercibimiento”

SEXTO: Con fecha 10/03/2021 se presentan por el reclamado las siguientes alegaciones:

-Reitera las respuestas dadas en los antecedentes en el sentido de que *“el sistema informático de control de acceso no almacena la huella digital de los empleados sino que se guardan las minucias y el sistema genera un algoritmo que no es reversible y a través del cual no se puede identificar a la persona”*. No existe un dato personal.

-No existe un sistema de control de accesos *“de las personas que acceden a los aseos” ni tampoco se controla acceso a cualquier otro lugar de la empresa que se citan en la resolución sino que el “sistema de control de acceso se limita a permitir el acceso de aquellos usuarios que constan registrados en el sistema de la empresa”, “ sin controlar ni la persona ni el tiempo que se permanece en esa ubicación” y “sin almacenar ningún tipo de dato de carácter personal”*.

-El sistema de control de acceso mediante huella dactilar fue suspendido técnicamente con efectos 1/04/2020, si bien se reactivó parcialmente desde el 1/06/2020 solo el de acceso a la nave y que *“los controles de acceso a los lavabos están desactivados, siendo el último registro de uso, el efectuado los días 4 y 5/03/2020.”*

Adjunta un documento firmado por el Gerente de la empresa que presta el servicio de gestión y control horario al reclamado, que indica:

“La reclamada cuenta con cuatro dispositivos contratados para registrar la jornada en sus instalaciones a través de la huella dactilar, uno ubicado en la entrada que da acceso al centro de trabajo y “tres dispositivos abrepuestas instalados en sus lavabos”.

El 24/03/2020 recibieron del cliente solicitud de suspensión del contrato por causa de la pandemia COVID-19”, “Con fecha 1/04/2020 se hace efectiva la inhabilitación técnica de los dispositivos instalados y del acceso al software portal horario contratado.”

“Con fecha 1/06/2020, se recibe por parte del cliente solicitud de reactivación del servicio, si bien se verifica que los dispositivos ubicados en los lavabos recibieron su último fichaje los días 4 y 5/03/2020.”

SÉPTIMO: Con fecha 15/03/2021, se acuerda iniciar periodo de práctica de pruebas.

Se acordó:

1. Dar por reproducidos a efectos probatorios la reclamación interpuesta y su documentación, los documentos obtenidos y generados por los Servicios de Inspección ante el reclamado y las alegaciones al acuerdo de inicio PS/00010/2021 presentadas por el reclamado y la documentación que a ellas acompaña.

2. Además, se le solicita al reclamado responda o aporte:

2.1- Según consta en el expediente de sus informaciones

“La finalidad de estos marcadores era el control de presencia y la seguridad en el acceso a las instalaciones.”

“Sobre los nuevos marcadores de acceso a las instalaciones y a los servicios, en el año 2017 se instala un nuevo sistema de marcadores, el actual y vigente, con nuevos marcadores tanto para la entrada de salida de la nave como para el acceso a los servicios, implantando un nuevo software de tratamiento de datos en la nube.”

¿Si las personas para acceder a la nave y con el fin de control de presencia laboral-fichaje, lo hacen solo con la huella o tiene el añadido de la introducción de una tarjeta.? Caso de que así sea, indicar que tipo de tarjeta, contenido y datos almacenados.

Si sucede lo mismo para acceder a los lavabos, o sucedía hasta el 5/03/2020.

Se recibió su respuesta el 23/03/2021, manifestando que para acceder a la nave con el fin del control laboral horario se utiliza solamente la huella.

Manifiesta que en los “lavabos exteriores que dan directamente a la nave” no ha existido nunca ningún control de acceso electrónico.

Hasta 5/03/2020 y *“para el acceso a los vestuarios, al poner la huella en el dispositivo lector se abría la puerta de acceso al vestuario únicamente a los usuarios registrados”.*

2. 2- Según su información, el sistema de acceso a lavabos es distinto del de acceso por fichaje, pues pretende por razones de seguridad que solo accedan los autorizados.

Sobre esto se le pregunta:

-¿Coinciden todos los empleados de la entidad con el número de autorizados, o se han de sumar mas personas?

Manifiesta *“que coincidían los empleados de la empresa con el número de usuarios autorizados con acceso a los vestuarios y a sus servicios internos, y no había autorizadas personas externas o ajenas a la empresa con acceso a vestuarios.”*

“El personal externo o ajeno a la empresa accede al lavabo externo mediante llave.”

2.3-Copia de la impresión de los últimos registros de acceso a lavabos.

Aporta copia archivo en pdf y señala que: *“de los meses de febrero y marzo de 2020 en el cual se puede comprobar que no se registraba el acceso a los lavabos exteriores y que por razones de seguridad solo se registraba el acceso a los vestuarios. “Desde 5/03/2020, los dispositivos de acceso a los vestuarios están desactivados, solo se registran los datos de entrada y salida de la nave”.*

El archivo aportado contiene

“informe fichajes”, 1/02 a 31/03/2020, contabilizando y actualizando el acumulado de horas de cada empleado. Figuran 65 empleados bajo el apartado Personal, 4 en Logística, 4 en J Equipo, 3 responsables y 1 Administración, total 76 sin el Administrador. Refleja “salida médico”, entrada o salida vestuario, cada una con un código, hora de entrada y de salida, fallecimiento familiar, incapacidad temporal por citar ejemplos.

Sobre el mismo, indica que se acredita que no se registran los accesos a lavabos, si a vestuarios, solo hasta 5/03/2020.

2.4-¿Que diferencia el sistema de acceso con huella a la nave, del sistema de acceso a lavabos, o que los diferenciaba hasta 5-03-2020? Indicar si no trabajan ambos con las huellas previamente registradas.

Manifiesta que el *“dispositivo lector de huellas ubicado en la entrada de la nave registra la hora de entrada de la hora de salida de la nave con la finalidad de llevar a cabo el registro horario.”*

“Hasta el 5 de marzo del 2020, la puerta de acceso a los vestuarios y a sus lavabos interiores estaba cerrada, el dispositivo lector de huellas que se hallaba ubicado en la entrada de los vestuarios tenía única y exclusivamente la función de abre puerta para los usuarios registrados, no tenía funciones de control horario”.

“en ningún momento se ha instalado ningún dispositivo ni se ha registrado el acceso a los lavabos exteriores”.

2.5 Indicar que datos se almacenan en los fichadores de los lavabos (según el certificado del encargado de tratamiento hay tres, indicar en un croquis donde se hallan) para que permitan la validación a través de la huella, y que relación tienen con las plantillas del fichaje presencial de entrada-salida.

Contesta que en los “lavabos exteriores que dan directamente a la nave no ha existido nunca fichadores.”

“Los tres fichadores de los vestuarios, uno de entrada y dos de salida no almacenan datos, son simples lectores que contrastan la huella con la minucia que el sistema tiene almacenado en la nube, sí coinciden el sistema abre la puerta”

Adicionalmente, puede aportar cualquier elemento probatorio que considere que el acceso con la huella del empleado autorizado, que se corresponde con empleado de la empresa no queda identificado como tal al acceder al lavabo, o no se conoce el nombre de la persona que accede.

Manifiesta que *“en los accesos al vestuario, una vez la persona está dentro del vestuario la empresa desconoce si acude al mismo para dejar o recoger alguna cosa de su taquilla o si acude al vestuario para utilizar sus lavabos interiores.”*

No aporta croquis que permita visualizar los espacios, los fichadores y las referencias que cita de vestuarios, fichador de vestuario, lavabo: fichador de lavabo de entrada en cada uno de los dos, y fichador de salida de cada uno de ellos.

2.6 Expliquen brevemente cómo se produce el sistema de registro y guarda-almacenamiento de la plantilla de las huellas, como se forma y donde se guarda la base de datos de algoritmos y que relación tiene con cada fichador, conexión, así como el de acceso salida a la nave como fichaje laboral y de los espacios destinados a accesos a lavabos.

Manifiesta que para dar de alta en el sistema a un nuevo trabajador, el Jefe de Personal se pone en contacto con el encargado del tratamiento y es este quien da de alta al operario en el sistema mediante un código y quien efectúa cualquier modificación en los fichajes. Esa empresa es la que guarda en sus servidores los datos. El reclamado no puede modificar ningún dato del fichaje de los empleados.

Aporta contrato con el encargado del tratamiento con fecha 25/05/2018 ya aportado anteriormente, y contrato con la misma entidad de 19/03/2021 de *“Servicio integral de Gestión de horarios”* en el que entre otros servicios: *“se facilitará el acceso a la consulta de fichajes, gestión de solicitudes, permisos y licencias, a través del Portal Horario”* al cliente. Acompaña



al citado contrato como parte del mismo el “*contrato de arrendamiento de datos y seguridad de la información servicio integral de gestión de horarios a través de la minucia de la huella.*”

Figura información referida a distintas modalidades de fichaje incluyendo el reconocimiento facial, unidad telefónica, fichaje al móvil por poner unos ejemplos, desconociendo cuál ha sido elegido.

Aporta copia de *registro de actividad* como encargado de tratamiento, indicando que prestan servicios de control horario mediante terminales de fichaje que transmiten a sus servidores centrales toda la información para ser tratada y a la que el cliente accede a través del portal Web con usuario y clave.

2.7 En sus alegaciones, en certificado de la empresa que presta el servicio, se indica que:

“La reclamada cuenta con cuatro dispositivos contratados para registrar la jornada en sus instalaciones a través de la huella dactilar, uno ubicado en la entrada que da acceso al centro de trabajo y “tres dispositivos abrepuertas instalados en sus lavabos”.

¿Si los abre puertas se refiere a que se debe introducir la huella tanto al entrar como al salir?, y ¿que diferencia existe en cuanto al uso y sistema de esta modalidad con la de acceso a la nave para fichar?

Manifiesta que la empresa tiene contratados cuatro dispositivos

- 1 acceso a la nave
- 2 acceso general del vestuario
- 3 salida de vestuarios masculinos
- 4 salida de vestuarios femeninos

Indica que solamente el dispositivo de acceso a la nave tiene una función de fichaje para el control horario. Los otros tres dispositivos tienen contenido abre puertas y no tienen funciones de control horario.

Desde 6/03/2020, solamente se encuentra activado el dispositivo del número 1, que mantiene las funciones de fichaje para control horario.

Se aprecia que no refiere aspecto alguno sobre los fichadores de entrada a lavabos puestos de manifiesto en la Inspección de Trabajo, aunque si señala la existencia de dos fichadoras de huella para la salida de los lavabos.

OCTAVO: Con fecha 5/10/2021 se emite propuesta del literal:

*“Que por la Directora de la Agencia Española de Protección de Datos se cambie la sanción de apercibimiento a la de multa administrativa, por la infracción de DAVISER SERVICIOS, S.L., con NIF **B43586809**, del artículo 5.1.c) 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), de conformidad con el artículo 83.5 a) del RGPD. Que la multa, en función de los artículo 83.2. a), b) y g) del RGPD y 76.2.b) de la Ley Orgánica 3/2018, de*

5/12, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es de 20.000 euros.”

NOVENO: Con fecha 20/10/2021, la reclamada efectúa las siguientes alegaciones:

1) Al resolver un acuerdo de inicio por una sanción de apercibimiento y la propuesta con una sanción de multa administrativa de 20.000 euros se vulneran los actos propios de la administración y se atenta contra el principio de confianza legítima.

Subsidiariamente, estima desproporcionada la sanción por:

La huella no permite identificar a la persona. No se almacenan los datos, no se produce afectación a ningún dato personal, los datos no son de categoría “esencial en el 2017”.

Los trabajadores fueron debidamente informados y colaboraron en la implantación. La finalidad es la protección de los trabajadores. No se ha irrogado daño alguno a los trabajadores

La empresa adopta medidas cuando es requerida por la Inspección de Trabajo. Colaboración en el marco del presente expediente.

2) La manifestación de que el apercibimiento no tendría carácter disuasorio carece de motivación.

3) El sistema de huella es habitual y ajustado a derecho y respetuoso con la doctrina jurisprudencial en cuanto a control de acceso a las instalaciones de las empresas a través de estos marcadores digitales, al considerarse que no revisten caracteres de intromisión ilegítima en la esfera de la intimidad.

Además, en este caso no se identifica al trabajador ni se conserva dato alguno susceptible ni tan siquiera de ser entendido como tal. Hacen referencia a la sentencia que aportan como documento 1, de la Audiencia Nacional recurso 774/2018 de 19/09/2019, fundamento de derecho V.

Indica que al instaurar el sistema en el año 2017, los datos biométricos no tenían categoría especial que le da el RGPD. No se le puede aplicar la normativa que figura en la propuesta de resolución y consideran que incluso el RGPD no instaura una prohibición absoluta respecto de su recogida y tratamiento siempre que esta sea adecuada pertinente y no excesiva en relación con el ámbito y las finalidades determinadas explícitas y legítimas para las que se han obtenido.

4) Incide en que no se produce un tratamiento de datos en el sentido estricto, y por lo tanto no se vulnerarían derechos de los trabajadores, pues considera que el sistema informático de control de acceso no almacena la huella digital de los empleados, sino que a través de una serie de parámetros aleatorios o minucias, el sistema genera un algoritmo que no es reversible y mediante o a través del cual no se pueden identificar a las personas solo permite saber que quien accede a los vestuarios no es una persona ajena a la empresa.

5) No es posible controlar a la persona que accede a los aseos, ya que el sistema se limita a permitir el acceso de aquellos usuarios que constan registrados en el sistema de la empresa, sin controlar con ello, la persona ni el tiempo que se permanece en esa ubicación.



6) En cuanto a los hechos probados, **lo subrayado no es correcto**, ya que o resulta acreditado lo contrario o la resolución se basa en suposiciones del instructor no contrastadas o atentatorios contra la documental.

a. (pág. 9), nunca esta parte ha indicado (ni se ha quedado acreditado) que existan pulsadores para entrar y salir del lavabo de modo independiente a la entrada al vestuario. Pese a ello, a lo largo de la resolución (ex. pág. 12 de la misma) se “*acusa*” a esta parte de no hacer mención “*deliberadamente*” a los pulsadores para acceder al lavabo femenino. No hay sistema de pulsador para acceder a los lavabos, ni femenino, ni masculino, (no hay un fichador adicional a la entrada del vestuario) sólo hay sistema de pulsador para acceder a sendos vestuarios, aparte del que existe para acceder a la nave”

b. Deduciones que carecen de sustento, se transcribe la resolución de la AEPD y **subraya lo que no ha sido acreditado** pese lo cual la resolución lo considera correcto: (pág. 10 Punto 4)“... Según se deduce de las manifestaciones el reclamado en pruebas, hay un acceso común para vestuarios a través del fichador que toma la huella, y desde el mismo interior se puede acceder por distintas puertas a vestuarios masculino o femenino. Considerando que para acceder a los lavabos hay un fichador, al menos en el femenino, en el que se entra con la toma de la huella, al que el reclamado no se refiere, los dispositivos o fichadores son según el reclamado:

1 De acceso y salida a la nave-para registrar la jornada de sus empleados en sus instalaciones a través de la huella dactilar, finalidad de control horario. Queda anotado en el registro automatizado-informe de fichajes diario de la empresa por cada trabajador, hora de entrada y salida, total de horas jornada y saldo horario.

2 De acceso general al vestuario (finalidad control de presencia, seguridad en el control de acceso a las instalaciones de la empresa) queda anotado también en el registro automatizado –informes de fichajes diario-por cada trabajador, la hora de entrada y salida durante la jornada-Desde el vestuario se accede registrando la huella a lavabos, aunque este fichador no es mencionado por el reclamado. Este acceso a lavabos no queda registrado en el informe de fichajes diario como tal. Para salir de lavabos es preciso registrar la huella, ignorando si se sale por donde se entró a vestuario, o es una salida independiente de la entrada a vestuario, en cuyo caso se estaría registrando en el informe diario de fichaje esta salida como tiempo en vestuario. Su finalidad, según el reclamado, es la seguridad de que acceda solo el personal autorizado, si bien antes de acceder a lavabo ya se habría pasado la toma de huella al acceder al vestuario.

c) (pág. 11) de la resolución se pretende erróneamente: “...El fin que se pretende es que solo accedan a aseos, personal autorizado, no externo a la organización. El reclamado ofrece información no muy clara al señalar que para las visitas existe otro espacio de lavabos que no coincidiría con el propio al que se accede a través de los vestuarios, tampoco indica cuantos vestuarios hay, si solo hay una entrada que conduce a dos vestuarios, omite que se tenga que introducir de nuevo la huella para acceder a los lavabos, y se desco-



noce si la salida de lavabos es a otro espacio distinto del vestuario. Estas cuestiones de toma de huella en estos espacios podrían conectarse en este caso con la cuestión de que los empleados tienen un tiempo de descanso programado durante el cual es el tiempo que han de acudir a realizar sus necesidades, si bien en ese caso la finalidad no era de control de las obligaciones contractuales, sino de seguridad de acceso a la instalación, si bien utiliza los datos de los empleados, por lo que mediatiza su uso para un fin genérico de seguridad de acceso.”

d) (Pág. 12) establece erróneamente que “..... El reclamado seleccionó el registro de la huella dactilar para el acceso a vestuarios y servicios. Su finalidad, de control de personas autorizada y por seguridad, que no tienen nada que ver con el control y vigilancia de las condiciones de cumplimiento del trabajo derivadas del contrato, ni con el cumplimiento de obligación legal impuesta al empresario. Estas razones de seguridad para el acceso en una parte de las propias instalaciones, no obstante, se reflejan como incidencia propia en el registro “informe horario” de fichaje de cada empleado, es decir, pasa a formar parte del registro de trabajo efectivo diario que se ha de considerar como el tiempo de puesta a disposición del trabajador frente al empresario y que es el objeto de lo que se ha de registrar como jornada.

El tiempo de estancia en lavabos, o momento de acceso-salida, según reclamado no se controla, no es su objetivo, si bien según su explicación, se toma la huella, pues están en el interior del vestuario que hay que franquear con huella. La cuestión es que el reclamado además, señala que les da un uso como abre puertas, cuando en realidad está, a través de esa actividad, tomando datos cada ocasión que se acceden esos espacios y se abandonan. Aunque nada diga del fichador adicional de entrada en lavabos, se toma la huella cuando se accede o sale de los aseos. De este acceso a aseos no queda reflejo en el informe horario de cada empleado, que queda englobado en el tiempo de vestuario, aunque el reclamado no da todos los detalles del fichador de registro a lavabo femenino. Así, con independencia de la implicación del registro, cada vez que se accede y se sale de aseos se tratan datos, aunque no se plasmen en el informe diario o queda más bien implícito en ese registro de tiempo de vestuario, se estarían tratando datos de tipo biométrico para dicha finalidad.”

1) Se remite a la documental obrante en el expediente y, además, acompaña como documento 2 a 4, varias fotografías, que manifiesta “ya obraban en el expediente” para mejor comprensión y acreditar que la disposición de la zona nada tiene que ver con la que recoge la propuesta. Las fotos no obraban en el expediente, pues eran otras tomas en la que no se indicaba a mano como ahora lo que es cada espacio ni se veía de frente.

En la foto DAVISER 2, se ve:

- a. De las dos puertas de debajo del reloj colgado en la pared, y una tercera que se veía en las fotos aportadas sobre el tema de la videovigilancia, esa tercera puerta, mas ancha, situada mas a la derecha del todo que al estar abierta parecía que conducía a otra nave, es la de un “vestuario, entrada y salida” según la anotación a boli.
- b. La puerta mas estrecha situada a la derecha de la que lleva una pegatina es según la anotación a boli que manda sobre la foto, es el “lavabo personas ajenas a la empresa”.



c. La puerta mas ancha, situada a la izquierda de la puerta con la pegatina de símbolo de aseo es otro “*vestuario, entrada salida*” según la anotación a boli.

En la foto DAVISER 3, tomada desde el interior de un vestuario, se ve que tiene solo un punto de entrada y salida, porque aparece anotado a mano con boli en la foto, figurando señaladas las puertas de dos baños en el interior del vestuario, que no disponen de fichador, “*baños sin control de huella*” señala la anotación, y no se ve que exista tal dispositivo.

En la foto DAVISER 4, tomada desde el interior del otro vestuario, (distinta disposición de la entrada) se ve que tiene solo un punto de entrada y salida porque aparece anotado a mano con boli en la foto, figurando señaladas las puertas de dos baños en su interior, que no disponen de fichador, “*baños sin control de huella*” señala la anotación, y no se ve que exista tal dispositivo.

Se ha de señalar que en pruebas ya se solicitó croquis con los espacios y aclaración de los espacios, y no fue aportado.

2) Sobre el “*documento aportado que refleja los tiempos de permanencia de los trabajadores en el vestuario (y lavabo, duchas, etc.)*” manifiesta que “*no computan a efectos de jornada laboral. “A efectos de jornada sólo computa el pulsador de entrada y salida de la nave.”*”

3) Propugna frente a la propuesta, que lo que se acredite sea:

“A. Hay dos vestuarios: uno para hombres y otro para mujeres. (documento 2 a 4).

B. No hay un acceso común para vestuarios a través del fichador que toma la huella, y desde el mismo interior se puede acceder por distintas puertas a vestuarios masculino o femenino. Existen pruebas que acreditan que existe una puerta para el vestuario femenino y otra para el masculino, y ambas, desde la nave. (documento 2 a 4).

C. No hay un fichador para acceder a los lavabos, ni al femenino, ni al masculino (documento 3 y 4), por lo que no puede concluirse como sí hace el instructor, que como sí habría una sistema de fichaje para el lavabo y por ello los fines del fichador serían ajenos al de seguridad. La huella sólo se debe introducir para acceder al vestuario de hombres y mujeres, no para acceder a sendos lavabos. Por tanto, no se ha omitido por esta parte que se debe colocar la huella para acceder al lavabo ya que no es así.

D. Los lavabos se hallan dentro de cada vestuario y sólo ha debido identificar la huella al entrar en el vestuario, no en el lavabo.(documento 3 y 4).

E. No hay un fichador de acceso al vestuario con la finalidad de control de presencia, ya que quedó acreditado que la jornada viene controlada sólo con el fichador de entrada y salida de la nave.

F. Se dice que se ignora si se sale del lavabo por donde se entró a vestuario, o es una salida independiente de la entrada a vestuario, cuando de la docu-



mental aportada quedó acreditado que la entrada y salida de cada vestuario es la misma (documento 2 a 4)

G. Entre la puerta de acceso al vestuario de hombres y de mujeres, hay dos puertas. Una privada y otra, que es el lavabo de terceros ajenos a la empresa al que para acceder deben pedir una llave (documento 2). Que exista un baño específico para personas ajenas a la empresa, (que quedó acreditado que sí acuden a la misma) refuerza que el sistema de identificación por huella es idóneo, necesario y proporcional y acredita que la finalidad del sistema no es otro que impedir que personas ajenas entren en los vestuarios de los empleados y responde a una medida de seguridad implantada por la empresa en beneficio de sus empleados.

H. Los trabajadores pueden acudir al lavabo y vestuario cuando tengan por conveniente, no tienen hora predeterminada ni tiempo máximo fijado para ello. A efectos de jornada sólo computa el pulsador de entrada y salida de la nave. Es decir, si un trabajador entra en el vestuario y permanece 8 horas dentro, ello no computa a efectos de jornada ya que constaría que ha trabajado desde la entrada a la salida de la nave. Esta realidad desvirtúa que la finalidad de los pulsadores de acceso al vestuario tenga la finalidad de control de jornada.

4) Concluye que:

-En cuanto a la afirmación que se contiene en el fundamento de derecho tercero página 14 en ese caso se produce el tratamiento de datos basado en el registro de la huella que permite identificar al empleado que accede al vestuario, lo que quedó acreditado es que:

1. *“El sistema de control de accesos no controla la persona que accede a los aseos, ni tampoco controla el acceso a cualquier otro lugar de la empresa, sino que se limita a permitir el acceso de aquellos usuarios que constan registrados en el sistema de la empresa, sin controlar con ello ni la persona ni el tiempo que se permanece en esa ubicación y sin almacenar ningún tipo de dato de carácter personal o identificable.”*

2. *El sistema informático de control de acceso no almacena la huella digital de las personas trabajadoras, sino que a través de una serie de parámetros aleatorios o “minucias” el sistema genera un algoritmo que no es reversible y mediante o través del cual no se puede identificar a la persona. Sólo permiten saber que quien accede a los vestuarios no es una persona ajena a la empresa.*

Los puntos anteriores desvirtúan el hecho probado último, el 7, para apoyar que no se lleva a cabo actividad de tratamiento.

- Que el sistema no afecta a la intimidad ni suponga intrusión alguna en la privacidad de los empleados y que se utilice para garantizar la seguridad de los empleados, corrobora:

1. El carácter necesario del sistema implantado, al no existir otro sistema alternativo, si se comparan los objetivos (finalidad) y el sistema en sí mismo, respetuoso con la privacidad de los trabajadores de los que no se toman datos que vulneren ningún derecho.
2. La idoneidad del sistema para la finalidad para el que se implantó (proteger a los trabajadores de presencias extrañas).
3. La proporcionalidad del sistema, máxime cuando no conlleva perjuicio o inconveniente o desventaja o vulneración de derecho fundamental alguno para los trabajadores.

Es función de la empresa garantizar la intimidad de los empleados, motivo por el cual, adoptar una medida distinta a la identificación mediante huella, podría conllevar que la empresa se viera sometida a denuncias con motivo de que los trabajadores encontrasen en el vestuario a personas ajenas a la empresa (un mínimo de cinco).

HECHOS PROBADOS

1) El reclamado manifestó en respuesta al traslado de la reclamación que implementó en el año 2017 un sistema de toma y registro de huella dactilar. Dispone de un único dispositivo digital o fichador que sirve para la entrada y la salida de la nave donde el personal accede para trabajar. “Para el acceso a los servicios” instaló otros tres marcadores digitales o fichadores, “ implantando un nuevo software de tratamiento de datos en la nube.”. “La finalidad es que accedan a las instalaciones “privadas de la empresa: servicio, el vestuario etcétera, sólo el personal autorizado para impedir el acceso a personal ajeno, como transportistas comerciales etcétera.”

2) El reclamado indica que el sistema implantado consta de cuatro dispositivos que funcionan insertando la huella digital de los empleados (marcador digital o fichadores), registrada previamente por el encargado del tratamiento del reclamado que gestiona el “servicio integral de gestión de horarios”. La actividad de registro y gestión de la huella se lleva a cabo a través de un contrato de encargado de tratamiento de 25/05/2018 con la empresa MHP SERVICIOS DE CONTROL SL, para la prestación de servicio integral de gestión de horarios a través de la minucia de la huella. Poniendo a disposición del encargado datos de los empleados, el encargado registra la huella de los empleados del reclamado que se procesa y se cifra mediante un algoritmo, quedando almacenados en servidores propiedad del encargado. El registro de actividad de tratamiento del encargado indica que presta servicios de control horario mediante terminales de fichaje que transmiten a sus servidores centrales toda la información para ser tratada y a la que el cliente accede a través del portal Web con usuario y clave.

3) De las fotos aportadas en la propuesta de resolución por la reclamada, archivos DAVISER 2, 3 y 4, se acredita que existen dos vestuarios-uno masculino y uno femenino- para el personal de la empresa, con un marcador digital o fichador común para acceder, siendo necesario introducir la huella digital del empleado. En el interior de cada vestuario existe un marcador digital o fichador en el que hay que introducir la huella para poder salir. Los vestuarios según las fotos aportadas disponen de taquillas, bancos. En cada vestuario hay dos

puertas en las que se accede al escusado o a la ducha, pudiéndose cerrar. No existe un marcador digital o fichador para el acceso propiamente dicho a este último espacio que comprende esas dos puertas en cada vestuario, por lo que el sistema de acceso y registro lo es a vestuarios/aseos. Las referencias a lavabo, servicios internos, que se hace previamente a la propuesta debe entenderse como un acceso a vestuarios/aseos para empleados, situado en la nave. Acceso a lavabo es acceso a vestuario/aseo. Para las visitas existe un *lavabo externo que no es otro que el situado al lado de los vestuarios, en una puerta que se abre previa petición de llave a la empresa*

4) Según el reclamado, visitan la nave donde prestan servicios sus empleados, unos cinco transportistas cada día, y ocasionalmente auditores de producto. En pruebas, el reclamado indicó que coincidían los empleados de la empresa con el número de usuarios autorizados con acceso a los vestuarios y a sus servicios internos, y *“no había autorizadas personas externas o ajenas a la empresa con acceso a vestuarios.”*, y que *“El personal externo o ajeno a la empresa accede al lavabo externo mediante llave.”*, lavabos que se distinguen de los internos de la nave, y que *“en ningún momento se ha instalado ningún dispositivo ni se ha registrado el acceso a los lavabos exteriores”*.

5) La Inspección del Trabajo acordó iniciar un acta de infracción el 14/12/2018 por denuncia de empleados, al comprobar que *“el marcador digital que abre la puerta existente para acceso a lavabo femenino”*, no funcionaba debidamente, requiriendo a la empresa una modificación del sistema de acceso a los servicios a fin de evitar incidentes contra la dignidad de una empleada. El reclamado implantó, para el caso de fallo de la huella en abrir lavabos, un pulsador a la entrada y otro a la salida. También se comunicó a los empleados que *“cualquier trabajador que precise acudir al lavabo fuera del horario de los descansos programados, se le comunicará al jefe de equipo o al superior jerárquico presente en el centro”* para poder sustituir al trabajador mientras tanto. El acta no determinaba que a los lavabos se accedía previamente por el vestuario y era antes de acceder cuando había que marcar la huella. El acceso a lavabos se debe referir pues al acceso a vestuarios/aseos como uno solo, uno para vestuario/aseos masculino, otro para femenino. Guarda relación con la afirmación que se contiene en la citada acta de infracción (*“el lavabo para lavarse las manos se accede después de fichar, por lo que obviamente es imposible fichar digitalmente con los dedos limpios.”*)

6) Los dispositivos, fichadores o marcadores digitales, son según el reclamado:

1 De acceso y salida a la nave (uno)- para registrar la jornada de sus empleados en sus instalaciones a través de la huella dactilar, finalidad de control horario. Queda anotado en el registro automatizado-informe de fichajes diario de la empresa- por cada trabajador, hora de entrada y salida, total de horas jornada y saldo horario.

2 De acceso general al vestuario (finalidad seguridad en el control de acceso a las instalaciones de la empresa, que accedan solo los autorizados, el personal que presta servicios para la reclamada) queda anotado también en el registro automatizado-informe de fichajes diario- por cada trabajador, la hora de entrada y salida durante la jornada-Al vestuario tanto masculino como femenino, se accede registrando la huella en un marcador digital o fichador común, uno. En el interior de los vestuarios que disponen de taquillas, bancos y dos lavabos, están los escusados, dos puertas en cada uno, que no tienen otro marcador adicional para poder entrar. Para salir de los vestuarios se sale por el mismo sitio que se entra,

para lo que de nuevo se ha de registrar la huella en un fichador situado en cada vestuario (total dos fichadores).

El reclamado manifestó en pruebas que el sistema de accesos con fichador digital para lavabos y vestuario, entendiendo que no son dos espacios distintos, sino vestuarios/aseos, dejó de funcionar con ocasión de la declaración de la pandemia, el 5/03/2020.

7) De acuerdo con el documento solicitado al reclamado en pruebas: “*informe fichajes*” de la empresa, 1/02 a 31/03/2020, el número de trabajadores asciende a 76. El registro de fichaje se actualiza, con el acumulado de horas de cada empleado, y refleja aspectos como “*entrada*” o “*salida*” de vestuario, indicando la hora a la que accede y a la que sale a lo largo de la jornada. La regla general es que se registra la entrada y no se registra a continuación entrada a vestuario/aseo como podría suceder si se ha de usar el mismo para el inicio del trabajo. Las entradas y salidas a o de vestuario/aseo, no se producen ni guardan relación con los momentos de la entrada o salida de la jornada. El reclamado ha manifestado en alegaciones a la propuesta que ““*A efectos de jornada sólo computa el pulsador de entrada y salida de la nave.*”

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

Los datos biométricos los define 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;

Resulta que los datos biométricos siempre pueden considerarse como “*información sobre una persona física*” ya que afectan a datos que proporcionan, por su propia naturaleza, información sobre una persona determinada. En el contexto de la identificación biométrica, la persona es generalmente identificable, porque los datos biométricos se usan para identificar o autenticar/comprobar al menos en la medida en que el interesado se distingue de cualquier otro.

En este sentido, cabe distinguir los supuestos de identificación biométrica de los supuestos de verificación o autenticación biométrica. La identificación es el proceso de reconocer a un individuo particular entre un grupo, comparándose los datos del individuo a identificar con los datos de cada individuo en el grupo (uno-a-varios). La verificación o autenticación es el

proceso de probar que es cierta la identidad reclamada por un individuo, comparándose los datos del individuo únicamente con los datos asociados a su identidad (uno-a-uno).

Los datos biométricos presentan la particularidad de ser producidos por el propio cuerpo y lo caracterizan definitivamente. Por lo tanto, son únicos, permanentes en el tiempo y la persona no puede ser liberada de él, no se pueden cambiar en caso de compromiso-pérdida o intrusión en el sistema.

Una utilización es amplia y sin control de la biometría es preocupante desde el punto de vista de la protección de los derechos y libertades fundamentales de las personas. Este tipo de datos es de una naturaleza especial ya que tienen que ver con las características comportamentales y fisiológicas de una persona y pueden permitir su identificación inequívoca

La aparente facilidad e inocuidad de la recogida de los datos de la huella puede provocar una falsa sensación de seguridad cuando es precisamente lo contrario. Dados los riesgos de reversibilidad de la huella, reconstrucción a partir de las huellas digitales encontradas en objetos, uso cada vez más frecuente de base de datos con interoperabilidad de los sistemas de tratamiento de huellas, falsos positivos que permitiría la admisión o el acceso indebido de sus usuarios que en realidad no están autorizados, o falsos negativos cuando el sistema no admite a una muestra autorizada, por lo que se hace preciso establecer unos principios y unas garantías específicas al respecto

Respecto a la sentencia alegada, de la Audiencia Nacional recurso 774/2018 de 19/09/2019, se trata de la sanción que la AEPD impuso al gimnasio FITNESS MURCIA PROMOTIONS SL, se dictó antes de la entrada en vigor del RGPD. En el fundamento de derecho IV se indica que los hechos “son de febrero 2017”, “con anterioridad a la entrada en vigor del RGPD” “que establece una regulación mas estricta al hallarse los datos biométricos dentro de las categorías especiales de datos.”

Conviene determinar la terminología técnica utilizada para una comprensión del asunto, en cuanto a las referencias que se producen en el contexto de la citada sentencia, de por ejemplo:

“La información biométrica se almacena en un algoritmo”.

“Minucias convertidas en algoritmos”.

“En efecto, aunque el registro de la huella se transforme en un algoritmo, el sistema se pone en marcha siempre y cada vez que el socio acude al gimnasio, poniendo el dedo en el lector digital lo que da lugar a la confrontación de datos con el algoritmo almacenado en los sistemas de la recurrente.

“Es decir, originariamente el funcionamiento del sistema está basado en la lectura de datos de la huella que se introduce en un terminal y en la confrontación con el algoritmo o secuencia numérica, que figura incorporado, que es un dato permanente y que está en una base de datos de la recurrente, el cual permite su asociación con la identidad de los socios. Por tanto, a partir de un dato único de cada socio que se transforma en algoritmo y que se verifica en cada entrada se están tratando datos del socio que accede al gimnasio y se permite su identificación.”

“En cuanto a la idoneidad de la medida, cabe señalar que la recogida y uso de la huella es para la prestación de un servicio, cual es el de acceso y uso del gimnasio y que el registro mediante huella dactilar consigue dicha identificación/seguridad que la persona que

accede al gimnasio es la que dice ser al poner el dedo en el lector y correlacionar su algoritmo registrado, por lo que con ella se consigue el objetivo pretendido y dicho juicio de idoneidad se cumple.”

“La entidad recurrente se ha preocupado por la confidencialidad con la conversión de la huella a su algoritmo y no han conservado en el sistema la huella o puntos de la misma sino el algoritmo”

“el algoritmo permaneciese bajo el control del usuario”

La AEPD ya lo ha puesto de manifiesto en la guía publicada “14 equívocos con relación a la identificación y autenticación biométrica” en su punto 1:” *la información biométrica se almacena en un algoritmo*” “Un algoritmo (RAE) es un método, un conjunto ordenado de operaciones o una receta y no un medio para almacenar datos biométricos. La información biométrica recogida (por ejemplo, la imagen de una huella dactilar) se procesa siguiendo procedimientos definidos en estándares y el resultado de ese proceso se almacena en registros de datos denominados firmas, patrones, plantilla o “templates”. Estos patrones registran numéricamente las características físicas que permiten diferenciar personas.”

Además la guía valora que la recogida de los datos biométricos puede revelar datos del sujeto como su raza o su género, su estado emocional, enfermedades, consumo de sustancias etc. , de modo implícito que el usuario no puede evitar como información suplementaria incorporada en su recogida. La guía ofrece links a estas afirmaciones que incluyen estudios científicos que concluyen en estas manifestaciones. Que los procesos de identificación o autenticación por sistemas biométricos no son precisos cien por cien como un sistema de contraseñas que o es o no es esa la contraseña. Los sistemas biométricos se basan en coincidencia o correspondencia de probabilidades, existen los falsos positivos, dan por buena una suplantación, o falsos negativos, rechaza a un individuo no autorizado. 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 basada en la información contenida en dichas bases de datos, y causaría asimismo un daño irreparable a los interesados. Por ejemplo, si las huellas digitales 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 de las huellas digitales, sin tener derecho a ello. Plantea una primera cuestión de prueba por parte del suplantado que se enfrentaría a un sistema técnico implantado por el responsable, y que podría suponer un robo de identidad, que (independientemente de su detección) quitaría fiabilidad a las huellas digitales de la persona para futuras aplicaciones y, en consecuencia, limitaría su libertad. Otros riesgos como caso de sufrir una brecha de seguridad son que si los patrones de la huella se almacenan cada vez en mas bases de datos, alcanza a mas individuos, el alcance del compromiso de los datos y su información para ser restaurado no es el mismo que si se produjera sobre el uso de contraseñas.

La sentencia alegada, por el marco normativo y el momento en que se dicta no tuvo en cuenta el avance y conocimiento de los riesgos inherentes a esta tecnología y sobre todo la excepcionalidad que prevé el RGPD, que por otro lado es una disposición ya dictada en 2016, si bien con una entrada en vigor diferida a 2018.

Para realizar el reconocimiento biométrico, las características biométricas se transforman mediante procedimientos técnicos en datos en diferentes formatos: una muestra (como la imagen de una huella dactilar, una imagen facial) y una plantilla (una forma reducida de la muestra traducida en códigos, números). Las plantillas biométricas se almacenan.

Los pasos técnicos del reconocimiento biométrico se pueden reducir a:

La primera etapa del tratamiento es la inscripción de las características biométricas en un sistema biométrico. Las características biométricas se «capturan» bajo la forma de una imagen, como una imagen dactilar. El formato resultante de esta fase se denomina muestra biométrica.

En una segunda etapa, la información contenida en una muestra se extrae, reduce y transforma en etiquetas o números a través de un algoritmo. Esta fase se llama extracción de características. Solo se conservará la «información discriminatoria destacada que es esencial para el reconocimiento de la persona». Las características extraídas se mantienen en una plantilla biométrica bajo la forma de una «representación matemática de la característica biométrica original». La plantilla es una reducción estructurada de una imagen biométrica: la medida biométrica registrada de una persona. La plantilla creada contiene las características personales de los parámetros capturados. Lo que debe almacenarse es la plantilla, presentada en forma digitalizada, y no el propio elemento biométrico. La plantilla de referencia se almacena para su comparación.

En una tercera fase, se comparará una muestra biométrica que se captura (como una punta del dedo) presentada en un sensor con una plantilla previamente grabada (como la plantilla de una huella dactilar).

Otro extremo de gran importancia desde el punto de vista de la protección de datos es el hecho de que algunos sistemas biométricos se basan en datos como huellas digitales o muestras de ADN, que se pueden recopilar sin que el interesado sea consciente ya que puede dejar rastros sin darse cuenta de ello. Al aplicar un algoritmo biométrico a las huellas digitales encontradas en un vaso, se puede averiguar si la persona está registrada en una base de datos que contenga datos biométricos, y en ese caso, determinar su identidad, mediante la comparación de las dos plantillas. Todo esto ocurre también con otros sistemas biométricos, como los basados en el análisis de la pulsación sobre las teclas o el reconocimiento facial a distancia, gracias a las características de la tecnología utilizada. El aspecto problemático es, por una parte, que esta recogida y este tratamiento de datos puede hacerse sin el conocimiento del interesado y, por la otra, que independientemente de su fiabilidad actual, esas tecnologías biométricas se prestan a una utilización generalizada a causa de su aparente inocuidad.

A partir de estas diferentes etapas técnicas y de la transformación de las características biométricas en información biométrica, pueden identificarse varias operaciones de tratamiento, tal como se definen en el artículo 4, apartado 2, del RGPD: en una primera fase (inscripción), se recopilan datos; durante la segunda fase (extracción de características), los datos se organizan, estructuran, adaptan y almacenan; la fase final de la comparación implica específicamente la recuperación, consulta, utilización y divulgación de los datos.

III

De partida, hay que destacar la nota del carácter restrictivo pues por principio, su tratamiento está prohibido y solo pueden aplicarse con carácter excepcional, en determinados casos enumerados en el RGPD.

El artículo 9.1 del RGPD parte de la misma posición, 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:*
 - a) *el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;*
 - b) *el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión 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”*

En este sentido, los considerandos 51 y 52 del RGPD lo ponen de manifiesto: *”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. (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. (...)”*

De este modo, estando prohibido su tratamiento con carácter general, cualquier excepción a dicha prohibición habrá de ser objeto de interpretación restrictiva.

El objetivo del reconocimiento a través de la huella digital es que desde la huella colocada en el terminal de entrada a vestuarios/aseos, encontrar una serie de puntos que coincidan con los patrones almacenados de la misma huella, en un conjunto de patrones almacenados en una base de datos, todo ello realizado en tiempo real. El funcionamiento se produce a base de reconocer internamente la huella que se le presenta en el fichador con las registradas en la base de datos. El contraste no se hace con la totalidad de la imagen de la huella que no queda registrada, pero si con el patrón de cada persona, que es único y contribuye al reconocimiento. Patrón extraído y almacenado en una base de datos donde se almacenan todos los patrones del personal del reclamado, es decir, en una base de datos centralizada. Cuando el empleado accede al sistema mostrando en el fichador, marcador digital o módulo de reconocimiento-hay varios en la sede del reclamado, y para distintos usos o finalidades-, su muestra que recoge en el instante, la compara, permitiendo la toma de decisiones en función del grado de similitud obtenido. Por tanto, en este caso, se produce tratamiento de datos, basados en el registro de la huella que permite identificar al empleado que accede a los vestuarios/aseos. Aunque no hay registro del acceso a aseos, por acceder desde el vestuario, si se considera preciso valorar que si se va al aseo, para abrir la puerta del vestuario que conduce a aseos, la obligación de introducir al entrar o salir un dato tan personal, permanente, invariable como la huella dactilar con los riesgos que conlleva el uso de dicho sistema. Ello, al hilo según el reclamado, de controlar que solo acceda el personal autorizado, refiriéndose a personas que no pertenecen a la empresa y podrían acceder a dichos espacios. No ha ofrecido mas explicaciones sobre estas razones de seguridad, deduciéndose por otro lado, que el aseo destinado a estos terceros, está situado cerca de los accesos a los vestuarios del propio personal, pero se franquea con llave que facilita la empresa.

Para poder utilizar este sistema, y para este fin concreto, de acuerdo con los parámetros establecidos en el RGPD, las empresas u organizaciones necesitan demostrar altos niveles de responsabilidad proactiva y diseño por defecto de Protección de Datos desde antes del tratamiento, incluyendo el hecho de ser capaces de justificar primero que hay causas para levantar la prohibición del tratamiento del artículo 9 del RGPD en datos biométricos que en este caso se basarían en razones de seguridad en los accesos a los vestuarios/aseos.

IV

Con independencia de que el uso de la huella para acceso a vestuarios/aseos, lo cierto es que se tratan los datos de la huella, y se hace en cada ocasión que se accede para realizar las necesidades fisiológicas diarias, y que además aunque no tenga una finalidad de control de presencia, lo cierto es que se refleja y forma parte del registro de jornada donde se cuentan los tiempos de entrada y salida del mismo. Cierto, que comparte espacio con el vestuario al que primeramente se accede, de modo que como manifiesta el reclamado puede acudir por distintos motivos a dicho espacio. Ahora bien, a ello añade que el tiempo transcurrido en vestuarios/aseos:

- *“no computan a efectos de jornada laboral. ““A efectos de jornada sólo computa el pulsador de entrada y salida de la nave.”, añadiendo*

- *“Los trabajadores pueden acudir al lavabo y vestuario cuando tengan por conveniente, no tienen hora predeterminada ni tiempo máximo fijado para ello. A efectos de jornada sólo*

computa el pulsador de entrada y salida de la nave. Es decir, si un trabajador entra en el vestuario y permanece 8 horas dentro, ello no computa a efectos de jornada ya que constaría que ha trabajado desde la entrada a la salida de la nave”

Lo que parece indicar es que a pesar de registrar en el informe de jornada el tiempo pasado por cada empleado en vestuarios/aseos, hora entrada, hora salida, no es necesario porque se considera tiempo trabajado, solo cuenta la entrada y salida, no interrumpe la jornada. Ello presupondría que no solo no se estimaría proporcional y necesario el uso del sistema de huella para este fin como se analiza en este caso, sino que la constancia de dichos datos no sería necesaria. Ese registro en la asistencia a vestuarios/aseos, cada vez que se accede y se sale de ese espacio, registra los datos y también los trata mediante el sistema de registro de huellas con una finalidad de seguridad en el acceso a los mismos.

En el presente supuesto, se considera que este sistema de acceso a vestuarios/aseos ha infringido el artículo 5.1 c) del RGPD, que indica:

“1. Los datos personales serán:

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)

En el considerando 39 también se reitera esa obligación:

“...los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios.”

En el registro de actividad del tratamiento del encargado, así como en el contrato de encargo de tratamiento no figuraba que la huella va a ser usada al mismo tiempo como medida de seguridad de accesos, para que terceros no accedan a dichos espacios reservados, o para que solo acceda personal autorizado. Dicho uso implica una distinta base legitimadora.

En este caso, se ha de valorar además en primer lugar, que el sistema utilizado sea idóneo para la finalidad, sea necesario, y proporcionado en su contexto específico, acreditándose que medidas técnicas menos intrusivas no existen o no funcionarían.

Esta triple valoración requiere una exhaustividad, partiendo como ya se ha dicho, no solo de la prohibición de tratamiento de estos datos, pues nos encontramos ante categorías especiales de datos personales, sino los riesgos de usar una tecnología intrusiva, los sesgos o la probabilidad de un error en la identificación, la suplantación de la identidad y el tipo de identidad única que contiene la huella, el impacto en la privacidad de las personas, las medidas de seguridad y la proporcionalidad o necesidad del citado tratamiento.

Ante el interés creciente en utilizar estos sistemas en ámbitos diferentes y, al tratarse de sistemas de identificación novedosos y muy intrusivos para los derechos y libertades fundamentales de las personas físicas, la constante preocupación de esta autoridad de control es compartida por el resto de las autoridades desde hace años, como ponen de manifiesto:

-El Documento de trabajo sobre biometría, adoptado el 1/08/2003 por el Grupo del 29,

-El Dictamen 3/2012, sobre la evolución de las tecnologías biométricas, adoptado el 27/04/2012, y que ha llevado a que el propio legislador comunitario incluya estos datos entre las categorías especiales de datos en el RGPD.

En este dictamen se 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”.*

-El Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del GT29 (adoptado el 8/06/2017) establece que *“aunque el uso de estas tecnologías puede ser útil para detectar o prevenir la pérdida de propiedad intelectual y material de la empresa, mejorando la productividad de los trabajadores y protegiendo los datos personales de los que se encarga el responsable del tratamiento, también plantea importantes retos en materia de privacidad y protección de datos. Por consiguiente, se requiere una nueva evaluación del equilibrio entre el interés legítimo del empresario de proteger su empresa y la expectativa razonable de privacidad de los interesados: los trabajadores”.*

Por ello, *“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. Esto puede formar parte de una evaluación de impacto relativa a la protección de datos (EIPD)”.*

Antes de implantar un sistema de reconocimiento de la identidad mediante la huella dactilar, el responsable debe de valorar primero si hay otro sistema menos intrusivo con el que se obtenga idéntica finalidad. El apartado 72 de la Guía 3/2019 del CEPD *“on processing of personal data through video devices”*, establece en este sentido que: *“The use of biometric data and in particular facial re cognition entail heightened risks for data subjects' rights. It is crucial that recourse to such technologies takes place with due respect to the principles of lawfulness, necessity, proportionality and data minimisation as set forth in the GDPR. Whereas the use of these technologies can be perceived as particularly effective, controllers should first of all assess the impact on fundamental rights and freedoms and consider less intrusive means to achieve their legitimate purpose of the processing”.*

(“La utilización de datos biométricos y, en particular, el reconocimiento facial conlleva riesgos mayores para los derechos de los interesados. Es fundamental que el recurso a dichas tecnologías tenga lugar respetando los principios de legalidad, necesidad, proporcionalidad y minimización de los datos establecidos en el RGPD. Considerando que el uso de estas tecnologías puede percibirse como especialmente eficaz, los responsables deberían, en primer lugar, evaluar el impacto en los derechos y libertades fundamentales y considerar medios menos intrusivos para lograr su objetivo legítimo de la transformación”. La traducción es de la AEPD).

Toda medida empresarial de control como esta de seguridad en parte de las instalaciones internas que conlleva el tratamiento de datos de carácter personal, que afecta a sus titulares, empleados y empleadas, para ser legítima, debe ser analizada desde el triple juicio de la:

-idoneidad: En este caso, el reclamado aprovecha en 2017 el uso de la huella para implantarlo con el fin de la *“seguridad en el control de acceso a las instalaciones de la empresa*. La seguridad en el acceso a vestuarios/aseos a través de la huella que pretende el reclamado puede servir para que no entren terceros a esos espacios que al no tener registrada la huella se verán impedidos, pese a que no acredite de origen la problemática que generan las visitas, si es que la generan, ya que disponen de un espacio propio para usar como lavabos. Una cámara además capta las imágenes de la puerta de vestuarios y del lavabo de visitas, que aunque también capta otro espacio mas amplio de la nave, se reconocería y se verían los accesos. Tampoco es el uso que de los citados datos se puede esperar según el RGPD.

-La necesidad del tratamiento, no debe confundirse con utilidad del mismo. Puede que se facilite el no tener que conocer o recordar la clave de acceso, llevar una tarjeta, es automático e instantáneo. Obviamente un sistema de reconocimiento por huella puede ser útil, pero no tiene por qué ser objetivamente necesario (siendo esto último lo que realmente debe estar presente). Como establece el GT29 - Dictamen 3/2012 sobre la evolución de las tecnologías biométricas- debe examinarse *“si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable”*.

En este sentido, la AEPD analizando la necesidad de un tratamiento concluye que, *“Si es necesaria o no, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia por poder llevarse a cabo manualmente la actividad. El termino necesidad no debe confundirse con útil sino si el tratamiento es objetivamente necesario para la finalidad”* -por todas, PS/00052/2020-.

La necesidad implica la necesidad de una evaluación combinada y basada en los hechos de la eficacia de la medida para los objetivos perseguidos y de si es menos intrusiva en comparación con otras opciones para lograr el mismo objetivo. Es también un principio de calidad de datos y una condición recurrente en casi todos los requisitos sobre la legalidad del tratamiento de datos personales derivados del derecho de Protección de Datos. Sí no hay necesidad objetiva del tratamiento, sí no es esencial para satisfacer esa necesidad, el tratamiento no es proporcional ni lícito.

En este supuesto, no se motivan las causas, motivos o circunstancias de porque en y desde 2017 y no se ha variado el sistema, se considera necesario mantener la seguridad de acceso a instalaciones internas y que se tenga que hacer con datos de los empleados y que además sean datos biométricos para el fin de control acceso a vestuarios/aseos a través de la toma de la huella, afectando a sus derechos y estableciéndoles mas tomas de datos cuando están simplemente ejerciendo sus derechos de acceso a espacios necesarios para el desempeño de sus funciones. La restricción de accesos se puede efectuar con otros

medios alternativos y no es ni constituye un área considerada de especial seguridad para requerir el grado de identificación que ofrece la huella, que no es pues indispensable para ejercer el control de acceso de terceros en este caso.

-Proporcionalidad, un vínculo lógico entre medida y objetivo perseguido. Además, para que una medida cumpla el principio de proporcionalidad, las ventajas resultantes de la medida no deben ser compensadas por las desventajas que causa la medida con respecto al ejercicio de los derechos fundamentales.

Para la realización de la valoración a la que acaba de hacerse referencia, el reclamado pone de manifiesto razones de seguridad en el control del personal a esos espacios. Cinco visitas aproximadamente cada día, frente a 76 trabajadores que han de utilizar cada ocasión que necesitan ir al lavabo entrar en los vestuarios/aseos. La reclamada cuenta ya con un control de acceso a la nave, y como personal ajeno a la entidad es en ese colectivo en el que se deberían de informar de las limitaciones, así como instaurar una modalidad subsidiaria de control para evitar accesos a zonas que tuviera en cuenta y respete la intimidad de los empleados.

El juicio de proporcionalidad conduce a que la adopción del sistema, considerando que fuera necesario, produjese una menor intromisión en el derecho, de forma que no pudiera existir un sistema igualmente eficaz cuya implantación implicase una menor injerencia en el derecho de los empleados. Y es en este punto donde nuevamente debe traerse a colación todo lo que se ha venido indicando en relación con la especial naturaleza que a los datos biométricos confiere el RGPD y que exige una especial atención no sólo a la proporcionalidad sino a la propia minimización del datos; es decir, que el dato sólo sea objeto de tratamiento en tanto éste resulte completamente imprescindible para el cumplimiento de la finalidad perseguida.

Hay que tener en cuenta como trasfondo de todo, que los lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos tienen una especial consideración en materia de protección de datos, no solo en instalación en su interior de dispositivos que permitan captar datos personales, por ejemplo videocámaras, por ser medidas directas de invasión de la intimidad de los empleados, estando prohibidos. A tal efecto, se ha de colegir que la colocación de dispositivos, en este caso que implican el tratamiento de datos biométricos, que controlan y pueden relacionar el acceso a dichas zonas, suponen una medida indirecta de control del acceso a dichos espacios, pudiendo relacionar por ejemplo el tiempo de permanencia, o el grupo de personas que permanecen en los mismos. Como regla general y dada la prohibición de este tipo de control, se han de instaurar otros medios para que el acceso a los mismos solo se produzca por el personal autorizado, que garantice la intimidad y el derecho del personal en un sistema proporcional que no sacrifique derechos fundamentales.

En este caso, además, las expectativas razonables del titular de los datos en el tiempo y en el contexto del tratamiento necesita ser cuidadosamente valorado. La monitorización sistemática y continua de la relación de los movimientos del empleado por el empleador afecta sin duda las expectativas razonables del titular de los datos. La interpretación del concepto de expectativa razonable debe no solo basarse en las expectativas del titular de los datos con respecto a su responsable, sino más bien al criterio decisivo de si se puede esperar razonablemente estar sujeto a una monitorización en una específica situación. La vigilancia de tales áreas o la monitorización es una intrusión intensa en los derechos de los sujetos. El legítimo interés del empresario en estos espacios salvo excepciones no prevalecerá sobre los derechos de los empleados. Se está produciendo una limitación de

derechos con la obligatoriedad de introducir la huella al entrar o salir de vestuarios/aseos sin que concurren la idoneidad, necesidad y proporcionalidad para ello. No existe acreditación de un fin legítimo para el control de accesos a esos espacios, ni se derivan de su implementación mas beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto

En el supuesto examinado el sistema de fichaje por huella para vestuarios/aseos no es el único con el que se puede lograr la finalidad pretendida al existir alternativas, sí que produce una injerencia no justificada en los derechos y libertades de los empleados reiterada y continuada.

Se acredita la inidoneidad y desproporcionalidad y no pertinencia ni adecuación del sistema de toma de huellas para acceder a **vestuarios/aseos con** la finalidad implantada de seguridad de acceso de personas a dichos espacios, por su insuficiente motivación, y generalidad, existiendo sin lugar a dudas métodos para que terceros ajenos a la empresa no accedan a esos espacios menos intrusivos que la toma de la huella en todas y cada ocasión que el empleado o empleada acuda por necesidades a dichos espacios.

V

Se observa también que tras el acuerdo de inicio, y la propuesta se han concretado los hechos a través de las pruebas y que con el mismo sistema aprovecha la huella para otra finalidad no laboral, que atenta contra los derechos de los empleados en la reiterada toma de sus datos cada vez que necesitan acudir a lavabos, entrada y salida.

Frente a la propuesta, la reclamada afirma que existían pruebas y constaban en el expediente pruebas que perfilaban claramente donde estaban los espacios de vestuarios, su relación con los lavabos o por donde se accedía y se salía. Los documentos que aporta como fotos en la propuesta (DAVISER 2, 3 y 4) en que se ven de frente y el interior los vestuarios y las dos puertas de lavabos interiores en cada vestuario, no obraban en el expediente, pues eran otras tomas en la que no se indicaba en ningún sentido y menos, a mano como lo hizo en propuesta, lo que es cada espacio ni se veía de frente.

En tal sentido, si que constan aportadas fotografías de marcadores, de puertas que se visionan, pero en ningún momento hasta después la propuesta se produce la identificación de esos aspectos, y los términos de referencia, tanto de la inspección de Trabajo, como de la reclamación y las alegaciones de la reclamada dan lugar al equivoco de que los fichadores están al acceder al lavabo, y por supuesto sin saber hasta ese momento ubicación y o entrada alguna de los mismos, o del destinado a visitas. Ello supone rectificar algunos aspectos referidos a la ubicación, la división de los espacios de vestuarios/ aseos que no afecta en lo esencial a la imputación y comisión de la infracción, ni a su carácter.

Bajo el motivo de seguridad del acceso a un espacio interno, en realidad, se están limitando los derechos con la toma de huellas en cada ocasión, quedando registrados sus datos. Ese medio de llevar a cabo el objetivo con la toma de huellas en todos los empleados no está justificado porque visiten diariamente cinco personas la nave, aduciendo razones de seguridad que no se desarrollan ni se relacionan con la necesidad del uso del sistema de la toma de huellas. También, el hecho de que en realidad los datos se toman de 76 personas, no de 30 como manifestó el reclamado, desconociendo la razón, sumando a ello la duración, desde 2017 con el incidente de 2018 en que intervino la Inspección de Trabajo acrecen en las razones a tener en cuenta para modificar la sanción de apercibimiento. Todas estas circunstancias se han de tener en cuenta de cara a la proporcionalidad y



disuasión de la imposición de la sanción. Considerando los mencionados elementos, la acción correctiva de la Agencia ha de tener en cuenta que en este caso no se consigue el carácter disuasorio de la sanción con un apercibimiento, dado que este análisis posterior alcanzado tras la instrucción, se aprecia y acredita que la naturaleza y gravedad de la conducta expresada es de mayor importancia de la que se tuvo en cuenta en el acuerdo de inicio. Todos estos elementos suponen que se varíe la imposición de apercibimiento por la de multa administrativa, de acuerdo con lo que prevé el artículo 58.2.i) del RGPD:

“i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso”

Las razones del cambio de sanción se detallaron en la propuesta, y la motivación aparece expuesta en la misma, sin que se deduzca indefensión material.

VI

El artículo 83.5 del RGPD indica:

“5. 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;”

Determina el artículo 72 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:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.”

VII

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. A fin de determinar la multa administrativa a imponer se han de observar las previsiones del artículo 83, apartado 2 del RGPD, que señala:

“2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

- b) la intencionalidad o negligencia en la infracción;*
- c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;*
- d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;*
- e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;*
- f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;*
- g) las categorías de los datos de carácter personal afectados por la infracción;*
- h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;*
- i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;*
- j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y*
- k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción”.*

Por su parte, en relación con la letra k) del artículo 83.2 del RGPD, la LOPDGDD, en su artículo 76, “Sanciones y medidas correctivas”, establece:

“1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

- a) El carácter continuado de la infracción.*
- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.*
- c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.*
- d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.*
- e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.*
- f) La afectación a los derechos de los menores.*
- g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.*
- h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado”.*

De acuerdo con los preceptos transcritos, a efectos de fijar el importe de la sanción de multa a imponer en el presente caso por la infracción tipificada en el artículo 83.5.a) del RGPD, de la que se responsabiliza al reclamado, se estiman concurrentes en calidad de agravantes los siguientes factores que revelan una mayor antijuridicidad y/o culpabilidad en la conducta del reclamado:

-La naturaleza, gravedad y duración de la infracción, considerando, especialmente los efectos que el tratamiento produce de manera continua en la privacidad de los trabajadores

afectados, en número de 76, desde 2017 (83.2.a RGPD).

-Aunque no se puede hablar propiamente de intencionalidad, el reclamante no tuvo en cuenta elementos adicionales de cumplimiento y garantía de derechos, ha centrado sus razones en parte en que no trataba datos biométricos, y sin cautelas ni medidas, por lo que es considerada clara y grave la falta de diligencia en la forma de actuar (83.2.b RGPD).

--Afectando a unos datos de carácter especial (83.2.g RGPD).

Como atenuante:

-El reclamado no es una entidad que tenga como objeto social o relacionado con el mismo el tratamiento de datos de modo habitual (76.2.b de la LOPDGDD).

Considerando los factores expuestos, la valoración que alcanza la multa por la infracción es de 20.000 euros.

Como medida adicional dentro del artículo 58.2.d) del RGPD es apropiada la conducente a dejar de tratar datos de toma de huella para entrar o salir en vestuarios/aseos, aunque la reclamada manifestó haberla llevado a efecto.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

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

PRIMERO: IMPONER a **DAVISER SERVICIOS, S.L.**, con NIF **B43586809**, por una infracción del artículo 5.1.c) del RGPD, de conformidad con el artículo 83.5 a) del RGPD, y a efectos de prescripción de la infracción en el artículo 72.1.a) de la LOPDGDD, una sanción de multa administrativa de 20.000 euros, de conformidad con los artículos 83.2.a), b), g y 76.2.b) de la LOPDGDD.

SEGUNDO: NOTIFICAR la presente resolución a **DAVISER SERVICIOS, S.L.**

TERCERO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29/07, en relación con el art. 62 de la Ley 58/2003, de 17/12, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº **ES00 0000 0000 0000 0000 0000**, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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 LPACAP. 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.

938-26102021

Mar España Martí
Directora de la Agencia Española de Protección de Datos