- **Expediente Nº: PS/00052/2021**

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, el reclamante) con fecha 3/07/2020 interpuso reclamación ante la Agencia Española de Protección de Datos (AEPD) La reclamación se dirige contra el **CONSORCIO PARA LA CONSTRUCCIÓN, EQUIPAMIENTO Y EXPLOTACIÓN DE LA SEDE ESPAÑOLA DE LA FUENTE EUROPEA DE NEUTRONES POR ESPALACIÓN** *con NIF* ***G95455473*** (en adelante, el reclamado). El reclamado declara que fue delegado sindical, pero ya no presta sus servicios para el reclamado. Los motivos en que basa la reclamación son que, desde noviembre 2019, el reclamado ha implantado en la empresa un sistema de control de presencia, fichaje horario por reconocimiento biométrico de huella. Se repartió entre los empleados un documento, identificado como 1, donde se requiere el consentimiento para el tratamiento de los datos biométricos y solicita que se determine si el reclamado ha actuado conforme a la legalidad vigente.

Aporta:

- DOCUMENTO 2, entregado por el reclamado, de tipo informativo, titulado "*ASPECTOS LEGALES DEL FICHAJE CON LECTORES BIOMÉTRICOS DE ROBOTICS* (empresa con la que contrataron el sistema) *QUE DEBEN SER COMUNICADOS AL PERSONAL", sobre las características de los sistemas biométricos de ROBOTICAS,* con el literal:

"*Desde el momento en que un usuario pone el dedo en el lector del terminal se genera un número de identificación. Este número es el que se almacena en la memoria del terminal y el que se distribuye a los demás terminales. Este mismo número es el que sirve para comparar si la huella corresponde a un usuario o no. Este número no tiene ningún valor fuera de los terminales de ROBOTICS, ni existe forma alguna de obtener una imagen a partir del mismo es decir no es reversible*"

-"*La AEPD determina que estos datos tienen la condición de carácter personal de categoría especial."* "*Los datos almacenados en los sistemas de ROBOTICS no contienen ningún aspecto concreto de la personalidad limitando su función a identificar a un sujeto cuando la información se vincula con este*."

-"*En cuanto a la necesidad de que el interesado preste su consentimiento o pueda oponerse al tratamiento de sus datos biométricos debe indicarse que el artículo 7 del RGPD-* 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);-*exige el consentimiento del interesado para cualquier tratamiento de sus datos de carácter personal incluidos los de categoría especial*". "*El tratamiento de datos biométricos queda amparado por el artículo 9.2 b) del RGPD al obtener el*

consentimiento explícito del trabajador o ser necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento -empresa -en el ámbito del derecho laboral y de la seguridad."

-"*En base al artículo 20.3 del Real Decreto por el que se aprueba la ley del Estatuto de los Trabajadores, la empresa podrá adoptar las medidas más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de las obligaciones y deberes laborales, en que el uso de datos biométricos para control de acceso a dependencias de la empresa es legítimo y no desproporcionado a la finalidad del tratamiento*."

"*En base al artículo 6 del RGPD el tratamiento será lícito mediante el consentimiento del interesado -empleado- o si el tratamiento es necesario para la ejecución de un contrato en el que interesado es parte*".

"*Es necesario que la empresa informe a sus empleados de todo lo anterior previamente al uso de dichos sistemas con el fin de facilitar dicha comunicación. ROBOTICS pone a su disposición una nota informativa que las empresas deberían entregar y hacer firmar a sus trabajadores en el momento de digitalizar sus huellas dactilares con el fin de poder acreditar ante una inspección que los trabajadores dieron su consentimiento expreso al tratamiento de datos biométricos*".

"*En conclusión, los datos biométricos de los sistemas de ROBOTICS permiten la identificación unívoca de individuos sin vulnerar sus derechos y libertades fundamentales."*

-DOCUMENTO 3, entregado por la empresa y firmado por ROBOTICS, titulado "*PROVEEDORES CONTRATADOS POR ROBOTICS CON ACCESO A DATOS*" que contiene tres empresas "*que tienen acceso a nuestros datos"*, una de ellas MICROSOFT IRELAND OPERATIONS LIMITED "*servicio SaaS*", y dos empresas españolas: servicio de gestión de tiques soporte, y plataforma formación "*e- learning*".

-Copia de correo electrónico del reclamante a la empresa, de **2/10/2019**, manifestándole que de acuerdo con una consulta que el formuló, la AEPD no considera preciso ni necesario el consentimiento en la implantación de la huella dactilar como sistema de fichaje, relacionado con el cumplimiento de las obligaciones.

Añade que los datos son biométricos, solicitando ser informado del tratamiento de sus datos, incluyendo la evaluación de impacto. **Acompaña** el documento de consulta firmado por la AEPD el 30/09/2019 en el que entre otras afirmaciones se señala que en el caso planteado, "*el empresario no debería recabar el consentimiento de los trabajadores para proceder a dicho tratamiento sino que este se basará en una base legitimadora distinta…"*

-DOCUMENTO 1, titulado: "*modelo de documento de consentimiento para el tratamiento de datos biométricos*", que es un formulario para cumplimentar y firmar por empleados que contiene una parte declarativa, y otra informativa, considerándose como "*prueba de conformidad".* El escrito declara que se *"consiente expresamente" "a digitalizar la huella dactilar con la finalidad de llevar a cabo el control de presencia de los*

empleados mediante reconocimiento biométrico en el que "*el sistema mediante autenticación biométrica no almacena una imagen de mi huella, sino un numero generado a partir de esta*." "*he sido informado de que el número almacenado a partir de mi huella se mantendrá activo en el sistema mientras perdure mi relación laboral* " también que "*no conservaran una imagen completa de la huella dactilar sino solo un número creado a partir de la huella. Dicho número no permite reconstruir la huella."* En el apartado de información se indica en legitimación:" *consentimiento del interesado*". El documento **figura fechado el 7/01/2020, nota de recibí**, indicando "*no consiento. Solicito la supresión de todos mis datos personales de cualquier registro, base de datos o similar de la empresa o terceros a los que se hayan cedido dichos datos*. "

SEGUNDO: En el marco de las actuaciones practicadas por la Subdirección General de Inspección de Datos, se traslada la reclamación con fecha 7/08/2020, con el literal:

"*HECHOS QUE MOTIVAN LA RECLAMACIÓN:*
El reclamante manifiesta que la empresa Consorcio ESS Bilbao ORG ha implantado un sistema de control de presencia mediante huella dactilar que no cumple con los parámetros establecidos por la normativa de protección de datos.

DATOS RELEVANTES:
Se aporta la documentación presentada con la reclamación.
Se deberá informar, con lo solicitado en el párrafo siguiente y en el mismo plazo, sobre la Evaluación de Impacto realizada y toda la información facilitada a los trabajadores.

En el plazo máximo de un mes, desde la recepción de este escrito, deberá analizar la reclamación y remitir a esta Agencia la siguiente información:

1. La decisión adoptada a propósito de esta reclamación.
2. En el supuesto de ejercicio de los derechos regulados en los artículos 15 a 22 del RGPD, acreditación de la respuesta facilitada al reclamante.
3. Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.
4. Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia.
5. Cualquier otra que considere relevante."

Con fecha 8/09/2020, se recibe respuesta, manifestando:

1) Firmaron el 24/05/2019 un CONTRATO con la empresa ROBOTICS, SA. Adjuntan copia del documento denominado "*propuesta*", "*PROYECTO DE IMPLANTACIÓN DE LA SOLUCIÓN "VISUALTIME" SaaS*" para la ESS Bilbao, oferta. Destacan como más significativos los siguientes puntos:

-El modelo en que se basa la solución *"VisualTime"* ofertada, es el de servicio integral o SaaS, "*software as a service*" que incluye todos los servicios necesarios para la puesta en marcha, las instalaciones de los componentes hardware, la activación de la licencia *"VisualTime",* el acceso web a sus supervisores para la explotación de la información y tratamiento, exportación e importación de datos a través del acceso web y

servicio de continuidad y mantenimiento para atender solicitudes y consultas, resolver incidencias y actualizaciones periódicas del software, copias de seguridad y Protección de Datos.

-El modelo funciona en una plataforma "*cloud"* con las ventajas de estar en la nube.

-Constan cuatro terminales.

-Figura en el *contrato de licencia de uso y servicios,* que *"VisualTime" es la aplicación en la que se almacenan los datos.* ROBOTICS, suscribió el contrato de alojamiento o servicios de "*cloud computin*g" para esta operación con MICROSOFT IRELAND OPERATIONS LTD (MIO) para la correcta prestación del servicio objeto de la licencia, que se considera también encargado de tratamiento en lo que respecta al funcionamiento del servidor. El cliente autoriza expresamente al proveedor a subcontratar con MIO los servicios de hosting *cloud computing* para la correcta prestación del servicio objeto de licencia, lo que supone el acceso y tratamiento de los datos contenidos en el fichero titularidad del cliente denominado "*recursos humanos"* por ambos terceros, otorgándose al proveedor la facultad de exigir contractualmente al subcontratista la implementación en sus instalaciones de las mismas medidas de seguridad por el implementadas previstas todas ellas en el RGPD.

-El ANEXO III, "*seguridad de datos","VisualTime""* SAAS informa que, entre otra información, que *ROBOTICS* tratará datos de carácter personal relativos a la identificación de los empleados del cliente, datos de empleo necesarios para ofrecer las soluciones contratadas y datos biométricos. Manifiesta el reclamado que tiene certificado de que cumple con los requisitos del Esquema Nacional de Seguridad,

-Existe un ANEXO IV dedicado a PROTECCIÓN DE DATOS (folio 50 del pdf "*proyecto de implantación*"). Se indica que el proveedor, ROBOTICS, es encargado del tratamiento y accede a los datos- propiedad del cliente como responsable del tratamiento- conforme a las instrucciones del cliente siempre en modo consulta lectura y otras referencias a cuestiones de materia de seguridad que ha de cumplir.

2) Manifiesta que ROBOTICS "*nos indicó que no se procede a un almacenamiento de la huella dactilar por su parte y que la aplicación de "VisualTime" no efectúa un tratamiento de datos personales especialmente sensibles, dado que los terminales de ROBOTICS no almacenan una imagen de la huella de los empleados, únicamente un número de muchos dígitos que se genera a partir de la huella. Es completamente imposible crear una fotografía o volver a obtener la huella de un empleado a partir de dicho número."*

Por todo ello, no se consideró necesario efectuar una evaluación de impacto en protección de datos, puesto que no se encontraba dentro de los supuestos recogidos en el Art. 35 del RGPD."

3) Aporta copia de DOCUMENTO 5.4. de "*seguridad de protección de datos personales*", de 10/06/2019, versión 01 en el que en "5.*Registro de tratamientos* "no se identifican o describen cuales son, mencionando las referencias legales, un apartado 9 de "*análisis de riesgos*" con las referencias legales, categoriza los tipos de riesgos y el sistema general de evaluación de riesgos de los distintos tratamientos que lleven a

cabo . El apartado 10:"*Evaluación de impacto*", enumera la normativa legal y los actores que participan en la misma. (archivo, parte dos, pág. 35/77). de "*nombramiento de delegado de protección de datos*" DOCUMENTO 5.4.2. con comunicación a la AEPD el 2/12/2019 y un "*Informe final sobre el proceso de implantación del sistema de Protección de Datos*" de 2/12/2019 con dos folios.

4) Considera que el tratamiento de estos datos *"es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del Consorcio ESS Bilbao en el ámbito del Derecho laboral y de la seguridad y protección social, de conformidad con lo establecido en el RD Ley 8/2019 del 8 de marzo, por el que se establece la obligatoriedad de las empresas de implantar un sistema de registro de jornada que debe incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada trabajador. A pesar de ello, el Consorcio ESS Bilbao decidió por principios de transparencia solicitar con anterioridad a su implantación el consentimiento de todos los trabajadores. Todos los trabajadores firmaron su consentimiento."*

El Consorcio ESS Bilbao *"realizó las debidas comunicaciones a toda la plantilla"(5.2 del documento)* en el que figuran correos electrónicos informando el 16, 23 y 27/09/2019 de:

-Implantación del sistema de control horario y registro de la jornada laboral. A partir del 1 de octubre se pondrá en marcha a modo de prueba durante un mes el sistema de fichajes *"VisualTime"* y " esperamos poner en marcha el sistema a toda la plantilla al 1 de noviembre".

- Se les remite:

-El documento emitido por ROBOTICS en relación con el cumplimiento en materia de RGPD ("*aspectos legales del fichaje con lectores biométricos de ROBOTICS que deben ser comunicados al personal*".

-"*Instrucciones de Jornada y horarios para ESS Bilbao acordados con los representantes de los trabajadores, así como el documento que certifica el cumplimiento del RGPD por parte de la empresa Robotics (suministradora del sistema de fichaje*)."

-Documento a rellenar sobre el consentimiento para el tratamiento de datos biométricos. "Detrás tenéis información detallada sobre la PD en lo que a control horario respecta".

La decisión sobre la implantación de este sistema de fichaje vino precedida por un periodo de consultas con los representantes de los trabajadores". Aportan:

-Copia de acta de reuniones mantenidas el **8/05, 23/09 y 18/11/2019** (DOCUMENTOS 5.3.1, a 5.3.3). (parte dos del archivo presentado, pág14/77)

- Se adjunta como DOCUMENTO 5.3.4. y entre la documentación se entregó un listado de proveedores contratados por ROBOTICS con acceso a datos (figura en DOCUMENTO 5.1.4.)

5) En archivo parte dos, (pág. 71/77), copia de informe de AUREN CONSULTORES SP, SLP de 4/09/2020 sobre el proceso progresivo de implantación del registro biométrico indica:

"Para valorar el alcance el tratamiento de datos realizado por ROBOTICS se analiza junto con el Consorcio:

-Las garantías ofrecidas por ROBOTICS en relación a las actividades a realizar -grado de cumplimiento con el RGPD y temas de seguridad de la información.

-Características sobre el sistema técnico utilizado para tratamiento de datos huella, que se efectúa mediante la aplicación comercializada por ROBOTICS "Visual-Time."

"*Teniendo en consideración la información recabada del proveedor ROBOTICS (designación de DPD, certificación en el Esquema Nacional de Seguridad, contrato de servicios con descripción de medidas de seguridad, etc.), y la documentación aportadas en relación a la aplicación "VisualTime" (escrito adjunto anexo), se consideró que el proveedor ROBOTICS ofrecía garantías en temas de protección de datos y seguridad de la* información, y que la aplicación comercializada *"VisualTime"* no efectuaba un tratamiento de datos personales especialmente sensibles. Por todo ello, no se consideró necesario efectuar una evaluación de impacto en protección de datos, puesto que no se encontraba dentro de los supuestos recogidos en el art. 35 del RGPD".

6) Aporta en el apartado 5.1 (archivo parte uno, pág. 16/73) "*información cumplimiento normativa protección de datos por ROBOTICS*", que se compone de:

- documento ya mencionado "*aspectos legales del fichaje con lectores biométricos de ROBOTICS que deben ser comunicados al personal*"

- esquema gráfico de "*Terminales-Esquema de comunicaciones"* con las fases:

- Alta de huella: "*el alta de la nueva huella se realiza en el terminal que genera y almacena un hash*". Una flecha que sale a una pantalla, indica" *"VisualTime" no almacena una imagen de la huella solamente almacena el hash generado*". Otra flecha que sale a otro dibujo indica: " *la validación de las huellas se realiza en el propio terminal que compara el hash almacenado en el terminal y envía a "VisualTime" un ID de usuario conforme su validez y tipo*."

-Distribución de huellas: una pantalla en la que indica *"VisualTime"* únicamente transmite el hash a los terminales autorizados.

-Eliminación de huellas, en un dibujo de la pantalla figura *"VisualTime"* elimina los datos de los terminales según autorización del empleado o baja definitiva

7) Aporta copia de hoja informativa de ROBOTICS titulado "*Nota informativa acerca de la protección de datos personales en los terminales*": "*Los terminales de ROBOTICS no almacenan una imagen del sistema biométrico que utilizan para identificar los empleados, únicamente generan un numero de muchos dígitos a partir del dato biométri-*

co utilizado. Es completamente imposible crear una fotografía o volver a obtener el dato biométrico de un empleado a partir de dicho número.
A efectos prácticos, esto significa que cada vez que usted se identifica mediante un dato biométrico en el terminal, se genera un número. El programa compara, luego, si este número corresponde a un empleado o no de la misma forma que lo haría con una tarjeta-."

TERCERO: La Directora de la Agencia Española de Protección de Datos acordó el 18/12/2020 admitir a trámite la reclamación presentada por el reclamante.

CUARTO: Con fecha 16/09/2020, se recibió escrito del reclamante en el que especifica que la denuncia consta de dos partes:

-La primera se refiere al uso de datos biométricos, que la empresa dice que no los almacena.

La segunda parte se refiere al hecho de que la empresa informe a los trabajadores de que sus datos personales van a ser accesibles por la empresa instaladora, pero no informa de que a dichos datos también podrán acceder otras empresas, como MICROSOFT.

Indica que la empresa tiene cuatro sedes (2 en Bizkaia, 1 en Álava y otra en Madrid) y que en las cuatro se da el mismo tratamiento de datos para todos los empleados.

Por otro lado, "*quisiera ampliar la denuncia: La empresa desde hace algunos años ha empezado a tramitar las nóminas con una empresa externa*." "*Dado que la información que ceden a dicha empresa creo que incluye datos personales de categoría protegida (sueldo, identidad, nº seguridad social, DNI…) creo que debería avisar a los empleados de que dichos datos van a ser compartidos con terceros. Nunca lo ha hecho. Se lo he señalado personalmente y no han hecho nada para solucionarlo*."

QUINTO: Con fecha 19/04/2021, la Directora de la AEPD acordó iniciar contra el reclamado, procedimiento sancionador de apercibimiento por por la presunta infracción del artículo 35 del RGPD, de conformidad con el artículo 83.4.a) del RGPD.

SEXTO: Con fecha 4/05/2021 se reciben alegaciones del reclamado, manifestando:

-En la elección del encargado de tratamiento para el sistema de registro de jornada laboral de los empleados tuvieron diligencia para escogerle, "*examinando los riesgos que implicaba el uso de dicho registro*" "*dotándose el mismo de medidas técnicas y organizativas adecuadas*", "contando con una certificación ISO 27001, aportan documento 1

- "E*ntendiendo ahora el criterio de la AEPD sobre el tratamiento de datos biométricos especialmente protegidos y la necesidad de elaborar una Evaluación de Impacto en el caso que aquí nos ocupa, procederemos a realizar la misma en la mayor brevedad posible*."

-Aporta documentación que ya ha sido aportada previamente:

-ANEXO III, "*seguridad de datos","VisualTime""*, que forma parte del contrato con ROBOTICS, (3/53).

-Documento consentimiento.

-Documento seguridad- protección de datos.(versión todavía 01, de 10/06/2019) que figura como referido en documento 5.4

SÉPTIMO: Con fecha 13/12/2021, se emite propuesta de resolución con el siguiente literal:

"PRIMERO: Que por la Directora de la Agencia Española de Protección de Datos se sancione a CONSORCIO PARA LA CONSTRUCCIÓN, EQUIPAMIENTO Y EXPLOTACIÓN DE LA SEDE ESPAÑOLA DE LA FUENTE EUROPEA DE NEUTRONES POR ESPALACIÓN, *con NIF* ***G95455473****, por una infracción del artículo 35 del RGPD, tipificada en el artículo 83.4 a) del RGPD, y a efectos de prescripción, en el artículo 73.t) de la LOPDGDD, con apercibimiento.*

SEGUNDO: Que por la Directora de la Agencia Española de Protección de Datos se proceda a imponer a CONSORCIO PARA LA CONSTRUCCIÓN, EQUIPAMIENTO Y EXPLOTACIÓN DE LA SEDE ESPAÑOLA DE LA FUENTE EUROPEA DE NEUTRONES POR ESPALACIÓN*, en el plazo que se determine, la adopción de las medidas necesarias para adecuar a la normativa de protección de datos personales las operaciones de tratamiento que realiza, con el alcance expresado en los Fundamentos de Derechos de esta propuesta de resolución."*

Con fecha 22/12/2021 se presentan alegaciones manifestando que al recibir la propuesta han cesado en el uso de la herramienta de uso de los daos biométricos como control horario, adoptando el sistema de control mediante tarjetas identificativas. Aporta copia de pedido de tarjetas de proximidad, fecha entrega 27/12/2021.

Solicita que no se imponga sanción.

OCTAVO: De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

1) El reclamado decidió iniciar en 2019 la implantación progresiva de un sistema control de presencia, fichaje horario por reconocimiento biométrico de huella.

2) El reclamado basa la licitud del citado tratamiento en al menos tres motivos:

-"es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del Consorcio ESS Bilbao en el ámbito del Derecho laboral y de la seguridad y protección social",(artículo 6.1b) del RGPD, "de conformidad con lo establecido en el RD Ley 8/2019 del 8 de marzo, por el que se establece la obligatoriedad de las empresas de implantar un sistema de registro de jornada que debe incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada trabajador" (6.1.c) del RGPD).

A pesar de ello, el Consorcio ESS Bilbao decidió por principios de transparencia solicitar con anterioridad a su implantación el consentimiento de todos los trabajadores (6.1.a del RGPD), indicando que todos los trabajadores firmaron su consentimiento, si bien el del reclamante no figura mas que el recibí el **7/01/2020**, con la nota de "*no consiento*".

3) El reclamado informó a la plantilla del sistema a implantar. También consta que se mantuvieron reuniones con los representantes de los trabajadores. Declara el reclamado que el sistema se iba a implantar en modo de prueba a partir del 1/10/2019 y para toda la plantilla a partir del 1/11/2019.

4) El reclamado aporta copia de contrato de encargo de tratamiento firmado el 24/05/2019 con ROBOTICS. ROBOTICS accede a datos del reclamado almacenados en el fichero "*recursos humanos*" conforme a las instrucciones del reclamado. Los datos se almacenan en la aplicación VISUALTIME, solución de software integral, en la que toda la infraestructura subyacente, el middleware, el software y los datos de las aplicaciones se encuentran en el centro de datos del proveedor. Para el almacenamiento de los datos, ROBOTICS tiene suscrito un contrato de alojamiento de "*cloud computing*" con MICROSOFT IRELAND OPERATIONS LTD que se considera subencargado del tratamiento en lo que respecta al funcionamiento del servidor.

5) El sistema de registro y uso de huella dactilar de los empleados, de acuerdo con el documento de ROBOTICS, denominado "*ASPECTOS LEGALES DEL FICHAJE CON LECTORES BIOMÉTRICOS DE ROBOTICS QUE DEBEN SER COMUNICADOS AL PERSONAL"* consiste en que: "*Se almacena un número generado a partir de características físicas de una persona*". "*Desde el momento en que un usuario pone el dedo en el lector del terminal* (disponen de cuatro), *se genera un número de identificación. Este número es el que se almacena en la memoria del terminal y el que se distribuye a los demás terminales. Este mismo número es el que sirve para comparar si la huella corresponde a un usuario o no. Este número no tiene ningún valor fuera de los terminales de ROBOTICS, ni existe forma alguna de obtener una imagen a partir del mismo es decir no es reversible*".

Sobre el alta de la huella, el reclamado indicó que " *se realiza en el terminal que genera y almacena un hash*". *"VisualTime" no almacena una imagen de la huella solamente almacena el hash generado*". " *la validación de las huellas se realiza en el propio terminal que compara el hash almacenado en el terminal y envía a "VisualTime" un ID de usuario conforme su validez y tipo*."

-Distribución de huellas: una pantalla en la que indica *"VisualTime"* únicamente transmite el hash a los terminales autorizados.

6) El reclamado cuenta con un documento de seguridad genérico, versión 1, de 10/06/2019, que aportó en su respuesta al traslado a la reclamación y en alegaciones a la propuesta, que contiene indicaciones genéricas para la seguridad de los tratamientos. El reclamado no dispone del documento de evaluación de impacto de protección de datos de los datos biométricos que trata en relación a su finalidad de control horario.

7) Tras la propuesta de resolución, el reclamado manifestó que ha cesado el tratamiento de la huella dactilar, cambiando al sistema de tarjeras de proximidad.

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 arts. 47 y 48.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

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

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;

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, o el posterior 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.

El artículo 9.1 del RGPD, indica:

" *Tratamiento de categorías especiales de datos personales*"

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

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

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 etc. A diferencia de una contraseña, en caso de pérdida no se pueden cambiar. Por otra parte, también existen riesgos evidentes si la tecnología utilizada no garantiza de manera suficiente que la plantilla obtenida a partir de los datos biométricos no coincidirá con la utilizada en otros sistemas similares. Es innegable que la utilización de sistemas basados en reconocimiento biométrico puede tener ventajas, como el registro de jornada, ahora bien, no parece que sea el único sistema que permita garantizarlo. Habrá que cuestionar si es necesario el tratamiento en relación con el fin que se persigue y la proporcionalidad objetiva del tratamiento. Estos elementos han de estudiarse junto con los principios informadores de la normativa que nos ocupa, para así poder determinar si las medidas implantadas son proporcionales a la intrusión en la esfera privada de los interesados que suponen.

La centralización de datos almacenados en servidores aumenta el riesgo de apropiación indebida de datos, así como la gravedad de las consecuencias de una potencial falla del sistema. A ello se añaden los productos que ofrecen los desarrolladores y diseñadores de productos relacionados con los datos biométricos, como el software y la verificación de su adaptación a estándares de seguridad existentes o que puedan surgir.

De acuerdo con la información proporcionada por el reclamado, al introducir la huella, se ha generado "*un número con muchos dígitos* " mediante la función hash (aplicación de un algoritmo) que proporciona un valor único. Lo que quiere decir es que la información biométrica recogida, en este caso, 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 o "*templates*". Estos patrones registran numéricamente las características físicas que permiten diferenciar personas. En el terminal o fichadora, se compara el patrón ofrecido cuando se introduce el dedo con el almacenado, en orden al registro de la jornada. Se estima que la comparación no se produce una contra una, la del empleado que accede con la suya, sino con todas las que están almacenadas, realizando una función de comparación uno a varios cada vez que se entra o sale. En este caso, aunque no se guarde enteramente la imagen de la huella, sino unos dígitos, cada una de ellas en la forma de plantilla, es capaz de identificar unívocamente a cada empleado al confrontar en el terminal la toma de la huella con el resto de las existentes. Las funciones que contiene el algoritmo permiten extraer los puntos característicos de la huella para su posterior comparación con una base de datos asociada al conjunto de usuarios previamente almacenado, siendo capaz de identificar a su titular de entre todas las plantillas, tratándose datos de carácter personal basados en el procesamiento de la huella, identificando de forma única a dicha persona.

Queda así, acreditado que el reclamado trata datos personales de carácter biométrico de sus empleados, en este caso con un fin de registro horario.

III

De la prohibición de partida del tratamiento de los datos biométricos y su excepcionalidad son muestra los considerandos 51 y 52 del RGPD, indicando: "*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. (...*)"

El RGPD prescribe las excepciones al tratamiento de los datos biométricos en su artículo 9.2, al indicar:

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;"

(…)

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud."

La LOPDGDD se refiere a estos datos de categoría especial en su artículo 9:

"1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679 , a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda."

La obligación del registro de la jornada laboral diaria de los empleados no procede de contrato, sino de una ley, el Estatuto de los Trabajadores, si bien su tratamiento mediante registro de huellas debería ser necesario en orden a dicha obligación, solo, "*en la medida*" en que así lo autorice el derecho, bien de la Unión, bien el de los Estados miembros, o un convenio colectivo, también en el marco del derecho del Estado, que contenga garantías adecuadas respecto a los derechos fundamentales y de los interés del interesado.

La correlación a esta mención se halla en el artículo 9 de la LOPDGDD, que señala:

En este sentido, el artículo 88 del RGPD ha establecido que los Estados miembros pueden, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y las libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular, entre otros, a efectos del cumplimiento de las obligaciones que establece la ley o por el convenio colectivo, la gestión, planificación y organización del trabajo. Estas normas deben incluir medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, en particular, en relación con, entre otros, los sistemas de supervisión en el puesto de trabajo.

IV

La limitación del derecho fundamental a la protección de datos personales debe ser la estrictamente necesaria. Ello implica que si la consecución de los fines previstos puede realizarse sin tratamiento de datos personales, será preferible esta vía y supondrá que no es necesario llevar a cabo tratamiento alguno de datos. Valorado que la recogida, almacenamiento y uso de datos es necesaria, que constituye per se una limitación del derecho de protección de datos, debe además cumplir con la normativa en cuestión. Ello requiere pues en primer lugar analizar y asegurar que la recogida de datos sea necesaria para la finalidad establecida o pretendida y si lo fuera, que sea proporcional.

La necesidad es un principio fundamental a la hora de valorar la restricción de derechos fundamentales, como el derecho a la protección de datos personales. Sobre el principio de necesidad de tratamiento de datos de carácter personal cabe decir que cualquier tratamiento de datos implica per se y de inicio, la restricción del derecho fundamental, al producirse la recogida y disposición de los mismos por parte del respon-

sable que va a operar con ello. Según la jurisprudencia, debido al papel que el tratamiento de datos personales desempeña para una serie de derechos fundamentales, la limitación del derecho fundamental a la protección de datos personales debe ser estrictamente la necesaria.

Antes de implantar un sistema de reconocimiento de la identidad mediante la huella dactilar, el responsable debe de valorar si hay otro sistema menos intrusivo con el que se obtenga idéntica finalidad. El apartado 72 de las Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de video, de 29 de enero del 2020, del Comité Europeo de Protección de Datos: "*El uso de datos biométricos y, en particular, del reconocimiento facial conllevan elevados riesgos para los derechos de los interesados. Es fundamental que el recurso a dichas tecnologías tenga lugar respetando debidamente los principios de licitud, necesidad, proporcionalidad y minimización de datos tal y como establece el RGPD. Aunque la utilización de estas tecnologías se pueda percibir como particularmente eficaz, los responsables del tratamiento deben en primer lugar evaluar el impacto en los derechos y libertades fundamentales y considerar medios menos intrusivos de lograr su fin legítimo del tratamiento*. "

El Dictamen 3/2012, sobre la evolución de las tecnologías biométricas de 27/04/2012, del Grupo de trabajo del artículo 29 (creado en virtud del artículo 29 de la Directiva 95/46/CE, órgano consultivo independiente europeo en materia de protección de datos y derecho a la intimidad. Sus cometidos se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE), indica que: "*Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar. Un tercer aspecto para ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado".*

Estas valoraciones requieren exhaustividad, partiendo en este caso, no solo de la prohibición de tratamiento de estos datos, 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, permanente e invariable que contiene la huella, su impacto en la privacidad de las personas, las medidas de seguridad, la necesidad y proporcionalidad o del citado tratamiento.

Respecto de la proporcionalidad ha señalado el Tribunal Constitucional en la Sentencia 207/1996 que se trata de "*una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad*."

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)".

De este modo, si dicha finalidad pudiera ser conseguida por la realización de una actividad distinta al citado tratamiento, sin que dicha finalidad sea alterada o perjudicada, debería optarse por esa última actividad, dado que el tratamiento de los datos de carácter personal supone, tal y como consagra nuestro Tribunal Constitucional, en Sentencia 292/2000, de 30/11, una limitación del derecho de la persona a disponer de la información referida a la misma."

En este sentido, debe recordarse el análisis efectuado por el Grupo de trabajo creado por el artículo 29 de la Directiva 95/46/CE, en el Documento de Trabajo sobre biometría, de fecha 1/08/2003, en que se señala lo siguiente:

"*Con arreglo al artículo 6 de la Directiva 95/46/CE, los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. Además, los datos personales serán adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente (principio de fines).El cumplimiento de este principio implica en primer lugar una determinación clara de los fines para los que se recogen y tratan los datos biométricos.*

Por otra parte, hace falta evaluar el cumplimiento de la proporcionalidad y de la legitimidad, teniendo en cuenta los riesgos para la protección de los derechos y libertades fundamentales de las personas y especialmente si los fines perseguidos pueden alcanzarse o no de una manera menos intrusiva.

La proporcionalidad ha sido el criterio principal en casi todas las decisiones adoptadas hasta ahora por las autoridades encargadas de la protección de datos sobre el tratamiento de datos biométrico....

El uso de la biometría plantea también el tema de la proporcionalidad de cada categoría de datos a la luz de los fines para los que se tratan dichos datos. Los datos biométricos sólo pueden usarse de manera adecuada, pertinente y no excesiva, lo cual supone una estricta valoración de la necesidad y proporcionalidad de los datos tratados. Por ejemplo, la CNIL francesa ha rechazado el uso de huellas digitales en el caso del acceso de los niños a un comedor escolar19, pero ha aceptado con el mismo fin el uso de los resultados de muestras de las manos. La autoridad portuguesa de protección de datos ha tomado recientemente una decisión desfavorable sobre la utilización de un sistema biométrico (huellas digitales) por parte de una universidad para controlar la asiduidad y puntualidad del personal no docente"

En el presente supuesto, se debería haber tenido en cuenta inicialmente, no solo como parte de la evaluación de impacto de protección de datos, sino como regla general en cualquier tratamiento un examen sobre:
-*idoneidad*: "*si tal medida es susceptible de conseguir el objetivo propuesto*". En este caso, el reclamado instaura progresivamente el sistema, pese a la advertencia del reclamante sobre la base legitimadora del consentimiento de los empleados, a la que luego se hará referencia, recabando el documento de consentimiento de todos. La limitación de los derechos de todos los empleados está frente al cumplimiento de una obligación legal laboral de registrar la jornada diaria, si bien los medios para ello que pueden ser variados, no tienen porque suponer la intromisión en los derechos de los empleados como sucede aquí. Es necesario aplicar, caso por caso, el principio de idoneidad con respecto a los fines perseguidos, lo que implica una especie de obligación de minimización de los datos por parte del responsable del tratamiento.

-La necesidad del tratamiento, es un requisito esencial que debe cumplir cualquier medida propuesta que implique el tratamiento de datos personales. Se justificará sobre la base de pruebas objetivas y es el primer paso antes de evaluar la proporcionalidad de la limitación. La necesidad también es fundamental a la hora de evaluar la licitud del tratamiento de datos personales. Las operaciones de tratamiento, las categorías de datos tratados y la duración de la conservación de los datos serán necesarios para el propósito del tratamiento.

La prueba de necesidad del tratamiento para cualquier limitación del ejercicio de derechos a la protección de datos personales ha de ser estricta, debiendo tratarse los mismos solo en los casos estrictamente necesarios, ya que en principio, cualquier operación de tratamiento de datos limita el derecho a la protección de datos personales, independientemente de que esa limitación pueda estar justificada. Esta necesidad como idoneidad para la finalidad del tratamiento debe estar justificada en la documentación de cumplimiento que el responsable debe disponer de acuerdo con el artículo 5.2. del RGPD, pudiendo contenerse asimismo en el documento de evaluación de impacto de protección de datos si concurren los elementos para realizarse.

La necesidad debe versar de si se tratan datos personales sobre la base de una evidencia objetiva, según los fines a determinar, si se precisan ineludiblemente esos datos personales o si la finalidad se puede cumplir sin tratar esos datos personales.

La necesidad implica que se requiere una evaluación combinada, basada en hechos, sobre la eficacia de la medida para el objetivo perseguido y sobre si resulta menos intrusiva en comparación con otras opciones para lograr el mismo objetivo. En este caso se trata de tratamiento de datos a través del registro de huellas para el cumplimiento de la obligación legal que se imponen al empresario del registro de jornada de cada trabajador en el artículo 34.9 del del Estatuto de los Trabajadores, norma que no prevé que se utilicen datos biométricos para ello. Los fines deseados son el registro de los datos, sin embargo el reclamado no abona la necesidad de implantar el registro de la huella para dicha finalidad ni que sea imprescindible indicando los motivos que su no uso impida obtener ese fin. Si el proyecto de medida no supera la prueba de necesidad, no es necesario examinar su proporcionalidad.

La necesidad no debe confundirse con utilidad del sistema. Puede que se facilite el no tener que 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 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.

-*Proporcionalidad*, La proporcionalidad es un principio general del Derecho de la UE. Restringe a las autoridades en el ejercicio de sus poderes al exigirles que logren un equilibrio entre los medios utilizados y el objetivo previsto. En el contexto de los derechos fundamentales, como el derecho a la protección de datos personales, la proporcionalidad es clave para cualquier limitación de estos derechos.

La proporcionalidad requiere 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. En otras palabras, la limitación del derecho debe estar justificada. Las salvaguardias que acompañan a una medida pueden respaldar la justificación de una medida. Una condición previa es que la medida sea adecuada para lograr el objetivo previsto. Además, al evaluar el tratamiento de datos personales, la proporcionalidad requiere que solo se recopilen y procesen aquellos datos personales que sean adecuados y relevantes para los fines del procesamiento.

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, es decir, se ha de valorar la proporcionalidad en su contexto específico, acreditándose que medidas técnicas menos intrusivas no existen o no funcionarían.

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.

Si no se cumplieran los tres requisitos señalados, se puede afirmar que la necesidad de acudir para el control horario a la toma de huella dactilar de los empleados no es imprescindible, pues existen otros medios que son aptos para ese objetivo. El sistema tampoco se ajustaría a los requisitos de proporcionalidad e idoneidad. Lo cierto es que en este supuesto no se aportado ningún análisis documentado sobre estos elementos, que como se ha indicado formaría parte esencial de la citada evaluación de impacto, cuya infracción es la que se considera cometida.

Por otro lado, el Supervisor Europeo de Protección de Datos, ha emitido entre otras, el 7/10/2020, una nota sobre el estado actual de la biometría, pudiendo ser consultado en https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/state-biometrics-wojciech-wiewiorowski_en.

V

En este caso, el reclamado indica que la base legitimadora del tratamiento, en función de las establecidas en el artículo 6.1 del RGPD, sería la del consentimiento expreso. Añade que existen otras dos, el cumplimiento de una obligación legal , 6.1.c) del RGPD y mantenimiento del cumplimiento de la relación contractual, 6.1 b), si bien la obligación no deriva del contrato sino de una norma. Así, por ejemplo, en el contexto laboral, deriva del contrato el tratamiento de la información sobre el salario y los datos de la cuenta bancaria para que pueda abonarse el sueldo, de modo que exista un vínculo directo y objetivo entre el tratamiento de los datos y la finalidad de la ejecución del contrato. El registro de la huella dactilar para el cumplimiento de la obligación de registro de jornada como lo plantea el reclamado, caso de cumplir los requisitos previos no es necesario para la ejecución del contrato sino en su caso lo sería para el cumplimiento de una obligación legal que se ha de adecuar a los principios generales de tratamiento de datos, previa superación de la prohibición del tratamiento por las causas tasadas en el artículo 9 del RGPD

No obstante lo dicho, el consentimiento en el seno de una relación laboral es una base legitimadora excepcional por:

-La propia definición del consentimiento, "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*" no se parte de una posición de equilibrio en la relación. Como ha subrayado el GT29 en diversos dictámenes, el consentimiento solo puede ser válido si el interesado puede realmente elegir y no existe riesgo de engaño, intimidación, coerción o consecuencias negativas importantes (por ejemplo, costes adicionales sustanciales) si no da su consentimiento. El consentimiento no será libre en aquellos casos en los que exista un elemento de compulsión, presión o incapacidad para ejercer la libre voluntad.

-El hecho de que puede ser retirado cuando lo desee su titular , elemento que se debe incluir en la clausula antes de que se preste, contando con que la retirada del consentimiento no conllevará ningún coste para el interesado y, por tanto, ninguna desventaja para quienes retiren el consentimiento.

-Debe darse la posibilidad de no otorgarse el mismo, y por tanto ofrecer alternativas.

-Los artículos 16 a 20 del RGPD indican que (cuando el tratamiento de datos se basa

en el consentimiento) los interesados tienen derecho a la supresión de los datos cuando el consentimiento se ha retirado.

VI

Se imputó al reclamado que, tratando datos de carácter personal de categoría especial, y existiendo la obligación de disponer de una Evaluación de Impacto en la Protección de los Datos Personales (EIPD) incumplió el artículo 35 del RGPD:

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

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

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

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

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

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

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

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

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

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

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

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

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

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

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

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

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

En desarrollo del párrafo 4, la Directora de la AEPD publicó una lista orientativa de tipos de tratamiento que requieren una evaluación de impacto relativa a la protección de datos , indicándose: "*En el momento de analizar tratamientos de datos será necesario realizar una EIPD en la mayoría de los casos en los que dicho tratamiento cumpla con dos o más criterios de la lista expuesta a continuación, salvo que el tratamiento se encuentre en la lista de tratamientos que no requieren EIPD a la que se refiere en artículo 35.5 del RGPD*." "La lista se basa en los criterios establecidas por el Grupo de Trabajo del Artículo 29 en la guía WP248 "*Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD*", los complementa y debe entenderse como una lista no exhaustiva:

"*4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.*

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

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

Al mismo tiempo, las Directrices sobre la evaluación de impacto relativa a la Protección de Datos y para determinar si el tratamiento entraña probablemente un alto riesgo a efectos del RGPD adoptadas por el grupo de trabajo 29, el 4 de abril de 2017, señala:

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

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

La finalidad de la evaluación de impacto, dentro del proceso del cumplimiento normativo "*accountability",* supone la toma de responsabilidad propia por lo que se hace con los datos personales y cómo se cumple con los principios, incorporando apropiadas medidas y registros para ser capaces de demostrar el cumplimiento. Las organizaciones deben demostrar que están cumpliendo con la norma, incluyendo medidas de documentación sobre como son tratados los datos, con que finalidad, hasta cuándo, y documentar los tratamientos y los procedimientos para centrar la cuestión desde un momento temprano de la construcción del sistema de tratamiento. Su implantación posibilita la minimización de riesgos en el momento de tratar los datos, teniendo en cuenta tal como se exige en la evaluación de impacto, la necesidad y la proporcionalidad de los mismos, la cantidad de datos, etc. Dentro de la EIPD, figurarían el inicial derecho y alcance que tiene de los titulares de los datos y valorando los riesgos, si existen garantías, análisis de como se ven afectados… para que antes de proceder al tratamiento se disponga de un documento que avale la gestión posterior, ayudando a identificar y minimizar los riesgos de un proyecto de tratamiento de datos que va a resultar o afectar en este caso en una alto grado de riesgo a los individuos, empleados del reclamado, dada la forma específica del tratamiento la naturaleza del contexto y los propósitos.

La implantación del sistema de registro horario sin realizar la preceptiva EIPD que correspondía en el caso concreto conforme a todo lo anteriormente expuesto, dado el alto riesgo que supone el tratamiento para los derechos y las libertades de los empleados, constituye una clara infracción del RGPD.

En cuanto a las medidas de seguridad que aporta el reclamado, las propias, que figuran en el documento 5.4 se debe indicar que solo son el marco general de actuaciones en cuanto al manejo de los sistemas de información y los criterios generales que se han de especificar para cada clase de tratamiento que se lleve a cabo. Se acredita no constando referencia alguna mas que al tratamiento de videovigilancia, y habiéndose implantado el tratamiento biométrico a partir de octubre 2019, el documento no recoge valoración alguna sobre el tipo de datos, la necesidad, proporcionalidad etc., aspectos documentales que deben concretarse.
En cuanto a las medidas que pudieran tener alguna incidencia en los riesgos recogidas en el contrato de encargo de tratamiento, en su ANEXO III, seguridad de datos, refiere la seguridad de los datos que se almacenan, sobre los que no se profundiza. Solo se indica que se implementarán procedimientos de actuación relativos a la seguridad técnica y organizativa del tratamiento de los datos y mantenimiento del secreto profesional utilizados con VisualTime SaaS, que garantizan la confidencialidad, integridad y disponibilidad de los mismos, el almacenamiento en la nube, así como las referencias terminológicas que se implementan usualmente literales sobre medidas de seguridad que ha de cumplir el encargo de tratamiento.

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

De la documentación obrante en el expediente y tal como se infiere de los hechos probados, no existen evidencias de la realización de la evaluación de impacto de protección de datos.

VII

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

las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;"

La LOPDGDD establece en su artículo 73.t):

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

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

VIII

El artículo 58.2 del RGPD dispone lo siguiente: "*Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:*

b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

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 particular;"

Indica el artículo 77 de la LOPDGDD:

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

…j) Los consorcios.

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

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

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

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

corresponda.

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

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

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

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

En cuanto a la alegación de no imponer la sanción, una vez iniciado, se continua el procedimiento de oficio, y se aprecia que la infracción estaba perfeccionada al momento de producirse la reclamación y de iniciarse el acuerdo. La subsanación de la infracción, en este caso puede permitir la no imposición de medidas de corrección o adecuación del tratamiento de datos de que se trata, pero no permite el archivo de la infracción como si no hubiese existido la conducta analizada.

Por lo tanto, de acuerdo con la legislación aplicable,

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

PRIMERO: SANCIONAR con apercibimiento a **CONSORCIO PARA LA CONSTRUCCIÓN, EQUIPAMIENTO Y EXPLOTACIÓN DE LA SEDE ESPAÑOLA DE LA FUENTE EUROPEA DE NEUTRONES POR ESPALACIÓN**, con NIF ***G95455473***, por una infracción del artículo 35 del RGPD, de conformidad con el artículo 83.4 a) del RGPD, y a efectos de prescripción en el artículo 73.t) de la LOPDGDD.

SEGUNDO: NOTIFICAR la presente resolución a **CONSORCIO PARA LA CONSTRUCCIÓN, EQUIPAMIENTO Y EXPLOTACIÓN DE LA SEDE ESPAÑOLA DE LA FUENTE EUROPEA DE NEUTRONES POR ESPALACIÓN**.

TERCERO: COMUNICAR la presente resolución al DEFENSOR DEL PUEBLO, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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 13/07, 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 LPCAP. 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