- **Expediente N.º: PS/00441/2021**

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 parte reclamante) con fecha 4/06/2021**,** interpuso reclamación ante la Agencia Española de Protección de Datos dirigida contra la CONSEJERÍA DE SANIDAD DE LA JUNTA DE COMUNIDADES DE CASTILLA-LA MANCHA con NIF ***S1911001D*** (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

"*El día 19 de agosto de 2020 cursé una denuncia ante la Agencia Española de Protección de Datos que constaba de DOCE Hechos perfectamente delimitados e independientes". "El 24 de septiembre de 2020 recibí notificación única y exclusivamente se refería al Hecho DOCE".*

"Del resto de Hechos hasta el momento no he tenido conocimiento."

SEGUNDO: Retomando la resolución del procedimiento por la reclamación de 19/08/2020, se ha de indicar que se resuelve en inadmisión a tramite el 24/09/2020, notificada al reclamante y no consta que contra la misma se interpusiera recurso.

La resolución de inadmisión, *expediente* E/07538/2020, indicaba en el encabezamiento:

"*En relación con la documentación que ha sido remitida a esta Agencia referida a MUTUA DE ACCIDENTES DE TRABAJO COLABORADORA DE LA SEGURIDAD SOCIAL 72 SOLIMAT le confirmo, en primer lugar, su recepción*."

"*La identificación de infracciones, por vulneración de medidas de seguridad o por ruptura del deber de confidencialidad, se vincula generalmente con casos en los que la documentación con datos personales hubiera sido expuesta fuera del ámbito de protección que suponen las instalaciones donde son tratados los datos o con la constatación de la existencia de una observación de los datos tratados por parte de terceros, no apreciándose en el presente caso indicios documentales suficientes que permitan deducir una vulneración del deber de confidencialidad o que las medidas técnicas y organizativas aplicadas por el responsable del tratamiento no sean las apropiadas para garantizar un nivel de seguridad adecuado al riesgo. No obstante, si dispone de documentos adicionales que puedan acreditar lo contrario puede presentar una nueva reclamación*."

También figura una anotación registral de "*denegación de teletrabajo solicitada por el reclamante el 15/02/2019*", entre otros motivos, porque por la naturaleza de los servicios prestados, requieren la presencia física del empleado y otros referidos en el artículo 2.2 del Real Decreto 57/2012 de 12/08 por el que se regula la prestación de servicios de los empleados públicos en régimen de teletrabajo en la administración de la Junta de Comunidades de Castilla la Mancha

TERCERO: Con fecha 8/06/2021, se recibe ampliación de la reclamación del 4 del mismo mes, indicando:

Añade sobre lo ya denunciado el 19/08/2020:

Sobre documentos 3 y 8 (resolución de teletrabajo de 25/06/2019 y citación en sede de Servicio de Prevención de Riesgos Laborales), le fueron entregados sin firmar, devolviendo los documentos, y le fueron entregados después para su firma en el despacho del Secretario Provincial (SP) en presencia de empleados, considerando se ha vulnerado su derecho a la confidencialidad respecto a sus datos.

Como hechos nuevos, pone de manifiesto:

a)-Las solicitudes de cualquier tipo, vacaciones, asuntos particulares, teletrabajo se realizan mediante la aplicación "*personal de cada funcionario" CHRONOS*, y pone de manifiesto por el correo electrónico recibido del SP el 7/08/2020, que concatena otro de un Jefe de Sección, que "*este funcionario "podría haber indagado en mi aplicación sin mi permiso"* (documento 13 y 14). Se trata de un correo del Jefe de Sección que le indica al SP: "*Con fecha 4/08/2020, el reclamante presenta a través de CHRONOS solicitud de permiso mediante teletrabajo para los días 5 y 6/08/2020 ""Con fecha hoy 5/08 estoy intentando rechazar la referida solicitud pero por problemas técnicos inherentes a la plataforma CHRONOS me esta resultando imposible*". Indica que ese día 5, "*su fichaje correcto estaba en color rojo*", "*que aparecen así cuando se han modificado a mano*". En el documento de registro de la aplicación 14 que aporta, figura la hora de entrada y salida, junto al añadido a mano, "*están en rojo*". "*Además, me han bloqueado unilateralmente las solicitudes de teletrabajo realizadas a través de la aplicación*. Aporta desde documento 15 a 27, pantallazos de dos días por semana, desde 25/09/2020 hasta 2/06/2021, considerando "*han accedido sin mi consentimiento"* el SP y un Jefe de Servicio. Señala que tiene concedido el teletrabajo desde 30/06/2020 por silencio administrativo, y le "*están poniendo trabas*", "*a fecha de hoy todavía no lo estoy disfrutando*".

b)-"He estado fichando hasta el 13/03/2020 con la huella digital datos biométricos, cuando hay otros medios de fichaje menos intrusivos". "No se me ha solicitado consentimiento". "No se ha informado del uso y finalidad de control horario" " y sobre todo que se iba a utilizar con fines sancionadores como se ha hecho conmigo". Aporta en documentos 5, 6 y 11 el relato de que diversos días de distintos meses, asistió al médico, y no se le ha computado como prestación efectiva de trabajo el tiempo de dicha asistencia.

c)-Con motivo de las restricciones de desplazamientos, al residir en otra localidad, tuvo que pedir un certificado contactando con la Secretaria de la Delegada, que le solicitó para elaborar el certificado el DNI y domicilio. Indica que la persona que desarrolla las funciones de la Secretaria no se corresponde con el puesto que dicha persona tiene adjudicado, que es de auxiliar administrativo, y no ha encontrado el cambio de una plaza a otra, y "*tengo dudas de que ocupe el puesto de Secretaria de la Delegada*", "*pudiendo haber accedido de forma fraudulenta a mis datos personales*".

d)-Con la entrega de documentos 51, 52, 54 y 56 recibí cuatro "i*nstruccione*s" dos primeras y última de la Delegada de Sanidad DS (14/05/2021, 16/10/2020 y 4/01/2021 y 13/05/2021) tercera del SP, entregados por el SP, "*arropado por*" la Secretaria de la Delegada en el

primer documento, por dos personas en el segundo, y otras dos en la tercera, cuyos nombres y puestos designa, indicando que son personas que no forman parte del Servicio de planificación, ordenación e inspección "*y entre sus funciones no se encuentra el acceso a ningún tipo de información confidencial"* sobre expedientes relacionados con la instrucción.

Los documentos son *nota interior*, *asunto*: "*instrucción orden de servicio*" en que se alude a la reestructuración comunicada el 10/05/2021, todos los integrantes del servicio en que se encuadra, le informan de la composición de su sección y funciones y colaboradores, y se le ordena impulse la tramitación de los expedientes que tiene a su cargo y se le adjunta la instrucción de 4/01/2021.

La segunda nota interior revisa las tareas del reclamante indicando expedientes en los que debe dar los tramites correspondientes, de acuerdo con el articulo 6 de la ley 40/2015 sobre instrucciones y órdenes de servicio, advirtiendo de que su incumplimiento puede dar lugar a corrección disciplinaria.

El resto son similares

e)-Vulneración del deber de secreto al enviar el ***PUESTO.1 el 4/11/2020 un correo electrónico sin copia oculta que cita al personal de la Delegación para practicarse una prueba serológica de la COVID 19, con la información que debíamos acudir, figurando un listado de nombres y apellidos de cada uno de los trabajadores, junto con fecha y hora, aporta copia en documento 53. El correo indica que "*adjunto fecha y hora de cita para aquellas personas que habiendo solicitado test rápido COVID 19 aun no lo tenían asignado*" y se le indica a cada empleado el día y la hora y sede. Comprende 83 personas y el citado Jefe de Sección, aparece relacionado con "*Sección de personal*."

f)-Falta de base legitimadora (art 6) para tratar el dato número de teléfono particular, que se vio obligado a proporcionar en base a la situación meteorológica producida en enero 2021, "*Filomena*", al desarrollar la prestación no presencial.

Aporta copia de un correo electrónico que le envía otro empleado el 10/01/2021. El e mail, partiendo de la instrucción 1/2021 de 9/01/2021 de la D.G. Función Publica motivada por la situación meteorológica existente, (dictada por la competencia atribuida en el Decreto 80/2019 de 16/07 por la que se establece la estructura orgánica y competencias de la Consejería de Hacienda y administraciones Públicas), y "*a la vista de que los interesados están expresando su voluntad de acogerse a la modalidad de prestación de servicios no presencial durante los días 11 y 12 de enero del 2021 debe aclararse dada la excepcionalidad de la situación así como la apremiante la necesidad que la motiva*", e interpreta y establece algunas condiciones de dicha instrucción. Indica que quienes se encuentran en las situaciones descritas por la instrucción deberán, aparte de solicitarla, "*estar a disposición del servicio, facilitando teléfono de contacto y atendiendo e mail corporativo, y en su caso conexión a control remoto VPN*"

CUARTO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), el 29/06/2021, se dio traslado a la parte reclamada, del literal:

"*El reclamante… expone que hasta el 13 de marzo de 2020 ha estado fichando con su huella dactilar sin que previamente le hayan informado del uso y finalidad del tratamiento*

que realizarían con sus datos personales, siendo estos posteriormente utilizados para sancionarle."

Y se solicita:

"…*Deberá analizar la reclamación, y remitir a esta Agencia la siguiente información:*

1.- La base jurídica del tratamiento y, en su caso, circunstancia que levanta la prohibición para tratar categorías especiales de datos, según el artículo 9 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)."

2.- La finalidad del tratamiento.

3.- Las garantías adecuadas implementadas para la protección de los derechos y libertades de las personas.

4.- Las categorías de interesados (trabajadores, clientes, usuarios, etc.) y la información facilitada a éstos sobre el tratamiento de los datos.

5.- La Evaluación de Impacto realizada o motivos por los que no se ha realizado (para conocer la lista de tratamientos de datos personales que requieren una evaluación de impacto, así como cualquier otra información relacionada con las evaluaciones de impacto, puede consultar la herramienta "Gestiona EIPD" en https://www.aepd.es/es/guias-y-herramientas/herramientas/gestiona-eipd)

6.- La decisión adoptada a propósito de esta reclamación.

7.- Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.

8.- Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia.

9.- Cualquier otra que considere relevante.

Deberá, además, aportar la documentación que figura en el Anexo I del presente escrito cuando los tratamientos se refieran a los supuestos que en él se contemplan.

ANEXO I

1) Si la reclamación está relacionada con la utilización de las huellas dactilares, deberá aportar la siguiente información:

- Descripción precisa del funcionamiento del instrumento utilizado para la captación de las huellas dactilares.

- Criterios utilizados para la codificación y el almacenamiento de la información captada (si los datos biométricos se almacenan en bruto o si son tratados de manera que sólo se almacena una plantilla biométrica).

- Motivos que justifiquen la necesidad y la proporcionalidad del uso de los datos biométricos para la finalidad perseguida.

- Medidas adoptadas para garantizar que no es posible la reutilización de los datos biométricos para otra finalidad."

Adicionalmente, se solicita en su punto 2, otro tipo de información si los datos fueran tratados con técnicas de reconocimiento facial.

QUINTO: Con fecha 29/07/2021, se recibe respuesta en la que manifiesta:

1- Señala la normativa que regula la deducción de retribuciones al personal empleado público por la parte de la jornada de trabajo no realizada, y que en la misma no se deduce que tenga carácter sancionador. Ese tratamiento está inscrito en el Registro de Actividades de Tratamiento (RAT), disponible en https://rat.castillalamancha.es/detalle/1006, denominado *gestión de personal de la Consejería de sanidad*, y como base jurídica la ley 4/2011 de 10/03 del empleo público de Castilla la Mancha y el Real Decreto Legislativo 5/2015 de 30/10 por el que se aprueba la ley del Estatuto básico del empleado público y el Real Decreto Legislativo 2/2015 de 23/10 por el que se aprueba el texto refundido de la de la ley del Estatuto básico de los trabajadores. Su finalidad es la gestión del expediente del personal adscrito a la Consejería, funcionario, eventual y laboral, control horario o de presencia del personal.

Tipos de datos: datos relativos a infracciones administrativas ,NIF, DNI, número de Seguridad Social, nombre y apellidos, dirección, teléfono, firma, correo electrónico, número de registro de personal ,huella. Otros datos: características personales, académicos y profesionales detalles del empleo económicos financieros y de seguros.

Manifiesta que la base jurídica del "*tratamiento de control horario*" se basa en los artículos 6.1.b), 6.1.c), 6.1.e) y 9.2.b), del RGPD.

2-Aporta la Secretaria General de Sanidad ANEXO 1, del que destaca:

La Orden de 7/09/2009 de la Consejería de Administraciones Públicas y Justicia sobre horarios de trabajo y vacaciones del personal funcionario señaló la duración de la jornada de trabajo, el horario fijo de presencia en el puesto de trabajo, y su supervisión. En su artículo 13 indica que "*todos los centros y oficinas de la administración de la Junta de Comunidades de Castilla la Mancha y de sus organismos públicos que cuente su plantilla con más de 15 personas deberán dotarse de los medios electrónicos o informáticos adecuados para el control del horario del personal. En todo caso, deberá garantizarse el cumplimiento de la normativa vigente sobre protección de datos de carácter personal*."

"*En la DPS de* ******LOCALIDAD.1****, desde ***FECHA.2 hasta ***FECHA.1, el sistema de control horario empleado ha sido el fichaje mediante comprobación de huella digital*. "

Alude a la normativa vigente en el momento en que se adoptó esa modalidad de

tratamiento, la Ley Orgánica 15/1999, de 13/12 de protección de datos de carácter personal (LOPD), que entiende de aplicación cuando se instaura el sistema, a la habilitación para ello al artículo 6 de dicha ley: " *No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento*…" .

Por orden de 5/12/2016, la Consejería de Hacienda y Administraciones Públicas, ejerciendo sus competencias sobre creación modificación y supresión de ficheros con datos de carácter personal de varias Consejerías de la Junta, determinó la creación del fichero *PERSONAL,* Diario oficial de CLM de 19/12/2016 en el que figura mencionado, "*para la gestión de los RRHH de la Consejería*", en tipos de datos personales que contiene, figura entre otros: "*huella*".

Con la entrada en vigor del RGPD, este fichero se transformó en un tratamiento que forma parte del RAT denominado: "*Gestión de Personal de la Consejería de Sanidad*".

"*Tras la resolución de la Dirección General de la Función Pública, (DGFP) de ***FECHA.3, por la que se amplían las medidas extraordinarias en relación con control horario del personal (aporta copia), los empleados desde el* ***FECHA.1** *pueden usar el ordenador de trabajo para realizar el fichaje de manera alternativa al dispositivo de control de huella digital, de acuerdo con la resolución de 10/05/2020 de la DGFP, que se publicó en la aplicación CHRONOS."*

La Resolución de 10/05/2020, de la DGFP, sobre medidas organizativas y de prevención de riesgos laborales para la reincorporación presencial del personal indica en su punto 4-B-8: "*En relación a la utilización de dispositivos de lectura biométrica para el fichaje, se continuará con la medida establecida el 13/03/2020 que posibilita realizar el fichaje mediante CHRONOS a través del ordenador de cada usuario o usuaria*", si bien se especifica que "*Todo ello, sin perjuicio de las especificidades y especialidades de la tipología de personal y servicios públicos a prestar por cada Consejería y Organismo Autónomo*".

3- Se adjunta copia del "*informe de la Delegación Provincial de la Consejería de Sanidad en* ***LOCALIDAD.1** *relativo a la información dada a los empleados públicos que toman posesión en la citada DP sobre el uso de los datos personales gestionados por la aplicación informática de control de horario del personal*" solicitado por la Secretaria General de Sanidad. El informe lleva fecha de 27/07/2021. Se indica en ANEXO III lo siguiente:

"En su momento (septiembre 2016) se colocaron en los diferentes tablones de la Delegación Provincial, a la vista de todo el personal, carteles informativos del nuevo sistema de fichaje (mediante huella digital), así como de la finalidad de los datos recogidos, de la existencia de un fichero a estos efectos, y de todas las demás previsiones de información recogidas en la normativa relativa a protección de datos vigente en aquel momento.

SEGUNDO.- Que los registros en la grabación de la huella digital de los empleados públicos fueron siempre efectuados por personal adscrito a la Sección de Personal de ésta Delegación Provincial (por el Jefe de Sección aproximadamente el 90% de los casos), quienes además informaron de la finalidad de los datos recogidos (control del cumplimiento

de las jornadas, control del horario y demás normas establecidas en la Orden de 7/09/2009, de la Consejería de Administraciones Públicas y Justicia, sobre horarios de trabajo y vacaciones del personal funcionario y normativa concordante establecida en el Convenio Colectivo aplicable en cada momento.

TERCERO.- Que durante la operación antes citada se dio la circunstancia que algún empleado público se negó a facilitar su huella digital, circunstancia ésta que se solucionó facilitando al empleado un código que este debe introducir en el terminal biométrico. En este caso el terminal recoge el código del empleado y la fecha y hora de entrada o salida.

3- Las garantías adecuadas para la protección de los derechos y libertades de los interesados, manifiesta que son las necesarias para garantizar el cumplimiento de los principios de protección de datos recogidos en el artículo 5 del RGPD. En el caso del control horario solo se utiliza para comprobar la presencia del trabajador en su lugar de trabajo durante el tiempo establecido por la Administración. "*Tal y como se ha indicado en el ANEXO 1, en caso de incumplimiento de horario se podrá reducir de la nomina la parte proporcional al tiempo no trabajad*o".

Los datos recogidos son adecuados, pertinentes y limitados a lo necesario para la finalidad, "*en el control horario, solo se recoge la fecha y hora de entrada/ salida y la identificación del empleado, pudiendo ser esta la huella dactilar si se emplea el terminal biométrico*".

5- El tratamiento tiene implantadas las medidas de seguridad que garantizan que los datos personales presentan los mínimos riesgos de seguridad, todo ello según el ANÁLISIS DE RIESGOS del tratamiento "*control horario*" de la Consejería de Sanidad, acompañan como copia de ANEXO IV, con las siguientes características:

a) Fecha 16/01/2021, "*versión inicial*", aprobado por "*responsable de protección de datos*".

Herramienta utilizada, "*GESTIONA"*, de la web de la AEPD, que se basa en respuesta de preguntas y que otorga un resultado sobre el nivel de riesgo, aceptable o no.

En el RAT, la finalidad es gestión de los "*RECURSOS HUMANOS DE LA CONSEJERÍA*:

-Colectivos afectados: empleados

-Tipos de datos: relativos a infracciones administrativas, NIF-DNI, nombre y apellidos, dirección, teléfono, firma, correo electrónico, número de registro de personal, huella otros datos características personales académicas y profesionales, detalles del empleo económicos y financieros y de seguros.

-Aplicaciones informáticas: *ACCESS MANAGER*, *FICHAR*, *CHRONOS*, *RENO* y *RENO WEB*

-Categoría valoración Esquema Nacional de Seguridad: media.

Para todas las tareas de control horario, la aplicación utilizada es *CHRONOS* que también almacena todos los datos en una base de datos tipo SQL Server.

Ciclo de vida de los datos: Dentro de cuatro fases (*1 captura de datos, 2 clasificación almacenamiento, 3 uso tratamiento, 4 cesión o transferencia de datos a un tercero para su tratamiento).* Se indica en la 1 "*captura de datos*", que los datos para realizar el fichaje se pueden recoger de las siguientes formas:

- Mediante la lectura de la huella dactilar en el terminal biométrico instalado en las entradas de los edificios. Se recoge la huella, y la fecha y la hora de entrada y salida.

- Mediante la introducción de un código facilitado al empleado y que este debe introducir en el terminal biométrico. En este caso, se recoge el código del empleado y la fecha y la hora de entrada y salida.

- A través del ordenador de cada empleado publico en la aplicación FICHAR *CHRONOS*

Riesgos identificados: Figura un cuadro con "*Amenaza/riesgo* " en el lado izquierdo y en su apartado derecho, "*Riesgo residual*", con el resultado bajo, medio. Destaca:

- *"Manipulación o modificación no autorizada de la información": bajo*

    - "*Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información*": bajo.

Finaliza indicando que el resultado obtenido es aceptable, "*por lo que cuando se implanten las recomendaciones realizadas el riesgo sería bajo*".

Se señala como recomendación:

"*Optar por sistemas de verificación o autenticación biométrica 1:1, utilizando la fórmula de combinar código más huella en todos los casos. Además, se recomienda que los sistemas se basen en la lectura de los datos biométricos conservados por la persona trabajadora, por ejemplo en una tarjeta*."

5-En documento aparte, ANEXO V, se aporta un escrito sin firma, fecha ni responsable en el que se indica:

"Informe de necesidad y proporcionalidad del control horario en la Consejería de Sanidad", indicando que la guía laboral de Protección de Datos publicada por la AEPD admite el uso de la huella dactilar como forma de identificación para el control horario de los trabajadores, siempre que se cumpla con todos los principios del RGPD.

Idoneidad: La medida permite lograr el objetivo propuesto.

El control horario mediante un sistema de huella dactilar consigue controlar la hora de entrada y salida del personal eliminando la posibilidad de suplantación de identidad del empleado.

Necesidad: "*No existe otra medida más moderada para la consecución de tal propósito con igual eficacia*".

El control de horario de los empleados públicos es *un tratamiento licito por parte de los servicios de personal de las Consejerías.*

A la hora de valorar la implantación de una de estas soluciones, se optó por introducir la identificación con huella dactilar ya que es una forma menos suplantable que las otras. Si se utiliza la huella dactilar, solo puede ser el propio empleado el que acceda al sistema de fichaje. Se decidió tras comprobarse el mal uso que se estaba dando a otros sistemas como tarjetas de identificación o códigos.

Por tanto, no existe ninguna otra medida que permitiera lograr este objetivo con el mismo nivel de eficacia.

Como consecuencia de la pandemia, desde los servicios de personal se ha habilitado una nueva aplicación, FICHAR, para que los empleados puedan fichar en su ordenador al empezar o terminar su jornada laboral, siendo recomendación de los servicios de personal la utilización de esta aplicación.

Proporcionalidad (la medida ofrece más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores de conflicto).

En este caso, procede ponderar si los beneficios son superiores al perjuicio que esta medida tiene no solo en el derecho a la Protección de Datos.

La utilización de la huella es una medida más racional y justa, ya que asegura el momento real en que el empleado ha entrado y salido de su lugar de trabajo. Además, el evitar posibles incumplimientos horarios por parte de un empleado es importante ya que puede dar lugar a que sean otros compañeros los que tengan que asumir su trabajo. Pese a que el uso de la huella supone un tratamiento más invasivo, los beneficios de este sistema no solo para el empleador sino para el interés público superan los perjuicios para este derecho. Además, el resto de las alternativas, uso de credenciales, de códigos, no impiden que se suplante la identidad del empleado."

6-El terminal biométrico cumple las especificaciones BioAPI (estándar ISO/IEC 19784); Las huellas se almacenan en una base de datos centralizada en SQL SERVER 11.

-"*Para la recogida de las huellas se usan terminales de control de acceso con sensores biométricos de la marca NITGEN-Fingkey Acces modelo SW101*". "*Estos terminales se conectan a un servidor central a través de la red corporativa. La huella se almacena en una bb.dd. centralizada en SQL Server 11 y se asigna para cada usuario al terminal o terminales desde los que puede fichar, no pudiendo fichar en ningún otro*".

-"*Tanto la codificación como el almacenamiento de las huellas, son realizados por la aplicación ACCESS MANAGER que es la que gestiona todas las transacciones de datos entre los terminales y la base de datos centralizada y sigue las especificaciones BioAPI (estándar ISO/IEC 19784). La aplicación es la que se encarga del cifrado cuya lógica queda totalmente oculta tanto al usuario final como al posible programador. ACCESS MANAGER no almacena huellas dactilares de los usuarios. La huella dactilar es transformada en un código a partir de un algoritmo, y posteriormente eliminada. Aporta pantallazo con imagen "mantenimiento de huellas" de ACCESS MANAGER en la que manifiesta "no existe ya ningún dato biométrico*."

- Sobre las medidas adoptadas para garantizar que no es posible la reutilización de los datos biométricos para otra finalidad, señala que las huellas son tratadas exclusivamente por la aplicación ACCESS MANAGER, desde la cual solo se pueden registrar o eliminar, en ningún caso copiar y mucho menos alterar. "*Las huellas se almacenan en una bb.dd. centralizada en SQL Server 11 con las mismas medidas de seguridad que el Servicio de Base de Datos tenga para el resto de bb.dd., es decir, forma parte de la infraestructura certificada (Conformidad ENS e ISO 27001). La codificación de la huella se realiza internamente y, al seguir el estándar BioAPI, los técnicos consideran que dificulta la reutilización de la huella en otros sistemas que no sean Nitgen*".

7- Sobre la Evaluación de Impacto, indica que se trata de un tratamiento que viene de la anterior normativa, el fichero de *PERSONAL* que tenía inscrito la Consejería de Sanidad en la AEPD. Se creó por la Orden de 05/12/2016, de la Consejería de Hacienda y Administraciones Públicas, de creación, modificación y supresión de ficheros con datos de carácter personal de varias Consejerías de la Junta de Comunidades de Castilla-La Mancha. (DOCM Nº 244 de 19/12/2016). "*Dicho tratamiento no ha sufrido ningún cambio tecnológico ni funcional que justifique la realización de esta EIPD*."

8-Sobre las causas que han motivado la incidencia que ha originado la reclamación, se remite al ANEXO I

9-Sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia, indica que en el tratamiento de datos para la gestión de personal y control horario, se va a incluir información en la aplicación *CHRONOS*.

SEXTO: Con fecha 12/08/2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

SÉPTIMO: Con fecha 4/04/2022, la Directora de la AEPD acordó:

"*INICIAR PROCEDIMIENTO SANCIONADOR a CONSEJERÍA DE SANIDAD DE LA JUNTA DE COMUNIDADES DE CASTILLA-LA MANCHA, con NIF S1911001D, por la presunta infracción del artículo 35 del RGPD, de conformidad con el artículo 83.4.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, (en lo sucesivo, LPACAP) la sanción que pudiera corresponder sería de apercibimiento, sin perjuicio de lo que resulte de la instrucción."

OCTAVO: Con fecha 21/04/2022 se reciben alegaciones, indicando:

1) Reitera que en el momento en que se puso en funcionamiento el sistema, la legitimación se halla en el artículo 6.2 de la LOPD:

2) El artículo 35.1 del RGPD cuya vulneración se imputa prevé que la EIPD sea antes del tratamiento y el principio de legalidad comporta la necesidad de predeterminación normativa de las conductas ilícitas y de sus sanciones. La subsunción de la conducta en el tipo predeterminado no es facultad discrecional de la Adminsitración.

"*En el presente caso, entendemos, que en el procedimiento sancionador iniciado, se podría estar vulnerando el principio de tipicidad, toda vez que el sistema de registro de la jornada laboral, mediante huella dactilar, se puso en marcha con anterioridad a la aplicación del RGPD, esto es, bajo la vigencia de la derogada Ley Orgánica 15/1999, de 13/12, de Protección de Datos de Carácter Personal, por lo que no cabría aplicar el punto 1 de artículo 35 del RGPD para iniciar el procedimiento sancionador por vulneración del mismo, pues ello iría en contra de lo establecido por el artículo 25.1 de la Constitución Española, que dispone:*

"1. Nadie puede ser condenado o sancionado por acciones u omisiones que en el momento de producirse no constituyan delito, falta o infracción administrativa, según la legislación vigente en aquel momento".

3) El acuerdo de inicio refiere que la EIPD se aplica a operaciones de tratamiento existentes que probablemente entrañan un alto riesgo para los derechos y libertades de las personas físicas y para las que se ha producido un cambio de los riesgos, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, y la reclamada considera que no se da ningún cambio en los riesgos desde su implantación, siendo una tecnología muy consolidada, "*plenamente conocida y utilizada por todo el personal de la Junta*".

4) Indica que a pesar de entender lo anterior, se va a realizar una EIPD de impacto con la participación de las entidades competentes (en materia de sociedad de la información y coordinación de la administración electrónica, encuadradas en la Consejería de Hacienda y Administraciones Públicas).

NOVENO: Con fecha 8/11/2022, se inicia un período de practica de pruebas, dando por reproducidos a efectos probatorios la reclamación interpuesta por el reclamante y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones previas de investigación que forman parte del procedimiento E/07369/2021.

Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por la reclamada, y la documentación que a ellas acompaña.

Se solicita a la reclamada que aporte o informe:

a) En su evaluación de riesgos indican:

-"*para el control horario una de las formas de captura de datos es la introducción de un código facilitado al empleado y que éste debe introducir en el terminal biométrico*".

A este respecto, se le solicita que informen si exclusivamente funciona con este código este tipo de accesos-no precisa huella dactilar- y qué empleados tienen la opción de utilizarlo, desde que fecha y hasta cuando.

- Se señala como recomendación:

"*Optar por sistemas de verificación o autenticación biométrica 1:1, utilizando la fórmula de combinar código más huella en todos los casos. Además, se recomienda que los*

sistemas se basen en la lectura de los datos biométricos conservados por la persona trabajadora, por ejemplo en una tarjeta."

Sobre la misma, motivos por los que no decidieron usar esta modalidad.

b) Si el control horario con huella fue interrumpido durante la pandemia, y actualmente, que sistema están utilizando.

c) Si la entidad utiliza el sistema de control huella dactilar para el control horario desde el ***FECHA.2, hasta ***FECHA.1, fechas desde las que comenzó a ser utilizado por el reclamante, y si cesó su uso el 13/03/2020, motivo, y si el reclamante utilizaba todos los días el sistema de huella dactilar. Motivos por los que se deja de usar en general el sistema de huella para control horario el ***FECHA.1, o si es optativo. Si así fuera, base jurídica usada e información proporcionada a los empleados.

Responde con fecha 7/12/2022, tras haberse enviado la propuesta de resolución el 2/12/2022

Manifiesta que "*la Resolución de la Dirección General de la Función Pública, de ***FECHA.3, por la que se amplían las medidas extraordinarias en relación con el control horario del personal de la Administración de la Junta de Comunidades de Castilla-La Mancha, dispuso la ampliación hasta el /07/2020 de la suspensión de las reglas de control horario establecidas en el artículo 13 la Orden de 7/09/2009 antes citada (prevista por la Resolución de la Dirección General de la Función Pública de 16/03/2020 durante la vigencia del estado de alarma), así como que a partir del ***FECHA.1, el fichaje se realizaría (obligatoriamente) a través del ordenador de cada usuario o usuaria (pues la aplicación corporativa CHRONOS permite esta técnica). Asimismo, en el informe antes citado se mencionaba que esta resolución fue objeto de adecuada difusión a todo el personal a través de su publicación telemática en el tablón de la aplicación corporativa CHRONOS*."

"*Por lo que respecta a esta Delegación Provincial, durante el período antes señalado por la Dirección General de Función Pública de suspensión de las reglas de control horario y fichaje obligatorio a través del ordenador (hasta 22-10-2021 como se verá en el siguiente párrafo), el terminal biométrico situado a la entrada del centro estuvo tapado con un cartel indicando la prohibición de su uso, al amparo de las citadas instrucciones y de la instrucción de servicio del Secretario Provincial específica en materia de Covid19, de 12-05-2020, donde expresamente se prohíbe la utilización del dispositivo de fichaje mediante huella y que el personal deberá marcar sus entradas y salidas utilizando su equipo informático a través de la aplicación CHRONOS*." Manifiesta que se adjunta la citada instrucción de servicio específica en materia de Covid19, pero no es aportada.

Actualmente, al amparo de la Instrucción 4/2021, de 22/10 de la Dirección General de la Función Pública, sobre control horario del personal empleado público de administración General de la Administración de la Junta de Comunidades de Castilla-La Mancha y sus Organismo Autónomos, a partir del 2/11/2021 el fichaje para el control horario se realizará a través de los dispositivos de lectura biométrica disponibles en cada centro de trabajo, sin que pueda realizarse a través del ordenador de cada usuario o usuaria (salvo para el caso del personal que tenga autorizada la prestación de servicios mediante tele-

trabajo). Se manifiesta que se adjunta la Instrucción 4/2021 antes citada, pero no es aportada.

d) En el informe de la Delegación Provincial de Sanidad aportado en el traslado de la reclamación, indicaron cuando se implantó la medida del uso de la huella dactilar para el control horario:

> *"TERCERO.- Que durante la operación antes citada se dio la circunstancia que algún empleado público se negó a facilitar su huella digital, circunstancia ésta que se solucionó facilitando al empleado un código que este debe introducir en el terminal biométrico. En este caso el terminal recoge el código del empleado y la fecha y hora de entrada o salida. "*
>
> Se le pregunta si durante la instauración de este sistema se daba la alternativa a los empleados para usar uno u otro medio, como lo justificaban y a cuantos empleados alcanzó, esta modalidad y porque no era ofrecida a todos.

Responde que "*en el momento en que en la sección de personal de la Delegación Provincial de la Consejería de Sanidad en* ******LOCALIDAD.1*** *se efectúa la grabación de la huella digital a todo el personal, se indica al mismo, si bien verbalmente, que en caso de fallo del sistema biométrico de marcaje mediante huella, pueden realizar el marcaje a través de la introducción de su número de DNI seguido a continuación de una clave de cuatro dígitos, por lo que todo el personal conoce que existe una alternativa al marcaje a través de la huella digital.*

Tan solo un empleado se ha negado al registro biométrico mediante huella digital y se le facilitó exclusivamente la alternativa de fichaje antes citada, tan solo dicho empleado público tiene habilitado exclusivamente el fichaje mediante código, y todos los empleados públicos pueden emplear el mismo como alternativa a efectuarlo mediante huella digital.

e) Manifestaron en traslado que:

"*Para la recogida de las huellas se usan terminales de control de acceso con sensores biométricos de la marca NITGEN-Fingkey Acces modelo SW101*"

Indiquen si esa afirmación es correcta o no sería la correcta que "*para la lectura de las huellas…"*

Responde que, " *consultado al servicio TIC*", "*han contestado*:""*Para la recogida de las huellas se utilizan tanto los terminales de control de acceso (Fingkey Access modelo SW101) como, en algunos casos, los dispositivos de recogida de huellas de sobremesa (Fingkey Hamster), ambos con sensores biométricos de la marca Nitgen. Los terminales de control de acceso se utilizan también para la lectura de las huella*s."

f) Manifiestan en el análisis de riesgos del tratamiento de control horario que cuando hay nuevos empleados públicos que se incorporan, se pone a su disposición diversas posibilidades, entre las que se incluyen la lectura de la huella, o la introducción de un

código, o fichaje desde el ordenador. Se le pregunta si se da a elegir entre cualquiera de los tres, y si sucede lo mismo con los que habían elegido la opción de huella dactilar o estaban obligados a usarla.

Señala que ya ha sido contestado anteriormente y que el marcaje desde el ordenador no está permitido desde la Instrucción 4/2021.

g) Papel que ha desempeñado la Delegación de Protección de Datos en la instauración del sistema de control de horario a través de la huella digital, en los cambios del RGPD, y en el documento de evaluación de riesgos.

Respondió que "*Este sistema de control horario fue instalado en 2016, cuando aún no existía Delegado de Protección de Datos*"

"*Respecto a la evaluación de riesgos, como consecuencia de la reclamación objeto de este periodo de práctica de pruebas, la DPD recomendó al responsable que se realizara una EIPD"* Aporta copia de un correo electrónico de 27/04/2022 en el que desde la unidad de protección de datos se informa a personal de la Junta, que es necesario realizar una evaluación de impacto del tratamiento de control horario, asociando personal de la DG Función Pública y representantes de la Consejería de Sanidad

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

"*El nivel de seguridad se establece en la configuración de cada terminal de acuerdo con el método de autenticación utilizado en el mismo:*
• El nivel de seguridad para la autenticación 1:1 está entre 1 y 9, y el valor predeterminado es 5.
• El nivel de seguridad para la autenticación 1:N está entre 5 y 9, y el valor predeterminado es 8.

Si el nivel de seguridad es demasiado alto, la tasa de fallos de autenticación puede aumentar, y si el nivel de seguridad es demasiado bajo, la tasa de errores de lectura puede aumentar."

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

Responde que: "Si no se reconoce la huella que se le presenta al terminal de control de acceso, el programa muestra un mensaje de error al usuario, no produciéndose el fichaje correspondiente. Si por plantilla del usuario se entiende la traslación matemática de la imagen de la huella dactilar que realiza el lector biométrico, ésta se almacena en la bb.dd. centralizada cuando la misma es recogida en el proceso de alta del usuario y es copiada a cada uno de los terminales de control de acceso en los que dicho usuario vaya a realizar sus fichajes. Las lecturas de huella que se realizan a la hora de fichar se utilizan para realizar la comparación con las almacenadas en el propio terminal y, en caso de coincidencia, registrar la identificación del usuario, así como la fecha y hora del acceso. Los usuarios tienen la opción de identificarse con su Identificador de AccessManager (que

hacemos coincidir con su DNI) antes de poner el dedo para el reconocimiento de su huella. En este caso el terminal solo coteja la huella recién leída con la almacenada para dicho usuario en el propio terminal".

j) Como garantizan que la plantilla biométrica extraída con el software adquirido es especifica solo para esa persona y no es utilizada por otros responsables del tratamiento de sistemas similares.

Responde que: "*desde las diferentes Consejerías, los usuarios de los servicios de personal, no tienen acceso a las plantillas. Pueden registrar huellas a través de la aplicación y en ese proceso pueden 'ayudar' a través de la aplicación a que dicha recogida sea lo más fina posible, pero en ningún caso pueden manipular la huella y mucho menos copiarla. Las plantillas solo son accesibles a nivel de bb.dd. Y las huellas que se leen a la hora de hacer el fichaje, no se almacenan, solo se utilizan para el cotejo con las plantillas*."

k) Se considera que cuando se utiliza el sistema de fichaje con huella, si se sale, se ha de marcar la huella, y si se vuelve ese mismo día se ha de marcar de nuevo. Indiquen como ha de hacer el empleado para justificar los diversos motivos por los que se puede ausentar del trabajo, aportando la instrucción o norma que se les hubiera dado a conocer.

Responde que "*Los motivos se implementan en CHRONOS, es decir, tiene que solicitar en la herramienta la situación que proceda en cada caso y ahí sí que hay un listado de motivos de ausencia de puesto de trabajo (registro de solicitud, conceptos) También que los justificantes se adjuntan por CHRONOS*."

l) Informen si con el cambio del RGPD se les proporcionó información a los empleados sobre los nuevos elementos de transparencia en el tratamiento de sus datos.

"*No, en el momento de la entrada en vigor del RGPD, pero como consecuencia de la reclamación, la DPD recomendó que se incorporase la información del artículo 13 correspondiente al tratamiento en la aplicación de control horario CHRONOS de la Consejería de Sanidad*",

m) Si han realizado ya la evaluación de impacto que manifestaban en sus alegaciones, copia de la misma o estado en que se encuentra.

La DPD junto con la Unidad de Protección de datos recomendó al responsable la realización de una EIPD, no solo del tratamiento del control horario, sino de los todos los tratamientos relacionados con la gestión de personal; por tanto, el alcance de la EIPD incluye todos esos tratamientos en los que existen dos responsables, la Secretaría General de la Consejería de Sanidad y la Dirección General de Función Pública.

Se recomienda que se haga así ya que según lo estipulado en los decretos de competencias, las Secretarias tienen la competencia para la "jefatura superior e inspección del personal de los servicios centrales y provinciales" y la Dirección General de Función Pública para "la elaboración de la normativa e instrucciones en materia de función pública, el asesoramiento jurídico y emisión de informes en el ámbito de sus competencias y el asesoramiento en materia de recursos humanos, así como la colaboración, asistencia y coordinación de los órganos con competencias en materia de personal."

"*realizando la evaluación de esta forma se podría extrapolar al resto de las Consejerías de la Administración regional con los ajustes que en su caso fuera preciso realizar en caso de tramitación de forma distinta de cualquier de los procesos*.". Aporta mensaje de reunión de 12/05/2022, indicando que se ha efectuado la descripción del ciclo de vida de los datos, si bien las reuniones no se llevan a cabo telemáticamente, sino por correo electrónico.

SÉPTIMO: Con fecha 2/12/2022 , se emite la propuesta de resolución con el literal:

"*Que por la Directora de la Agencia Española de Protección de Datos se sancione con apercibimiento a la CONSEJERÍA DE SANIDAD DE LA JUNTA DE COMUNIDADES DE CASTILLA-LA MANCHA, con NIF* ***S1911001D****, 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*."

OCTAVO*:* Con fecha 5/12/2022 la reclamada accedió a la notificación. Con fecha 20/12/2022, se reciben alegaciones en las que indica:

1) Reitera lo ya manifestado y solicita sean tenidas en cuenta las respuestas dadas a las pruebas.

2) Estima que el sistema de control con la huella dactilar, es proporcional pues no se ha encontrado ningún sistema que permita con la misma eficacia cumplir con el objetivo de controlar la jornada laboral del empleado publico, toda vez que este es el único que obliga al trabajador a desplazarse al centro de trabajo. Otros sistemas, como el de tarjetas, códigos o la firma, no garantizan que sea el propio trabajador el que fiche. Tampoco tienen la misma eficacia otros sistemas como el fichaje mediante ordenador, toda vez que el trabajador, como se ha comprobado en distintas auditorías realizadas, puede fichar desde otros dispositivos como el ordenador de casa, el móvil etc., y por tanto no cumple con la finalidad de controlar que el trabajador se encuentra realmente en su puesto de trabajo.

Por otra parte, el sistema de fichaje mediante el ordenador no es extensible a todo el personal, ya que hay empleados públicos que no disponen de ordenador. Además, se recibían muchas quejas de parte del personal por el tiempo que perdía desde que entraba al edificio, llegaba a su al ordenador personal, entraba en el programa y fichaba. Por todo ello, el sistema de fichaje mediante ordenador se sigue manteniendo en la actualidad únicamente para el personal que teletrabaja en los días en que lo hace.

3) Aporta copia de la Instrucción 4/2021, de 22/10 de la Dirección General de la Función Pública, sobre control horario del personal empleado público de la Admón. General de la Administración de la Junta de Comunidades de Castilla-La Mancha y sus OOAA, en la que destaca:

"Primero. A partir del 2 de noviembre de 2021 el fichaje para el control horario se realizará a través de los dispositivos de lectura biométrica disponibles en cada centro de trabajo, sin que pueda realizarse a través del ordenador de cada usuario o usuaria. Segundo. El personal que tenga autorizada la prestación de servicios mediante teletrabajo continuará registrando el tiempo de trabajo de cada jornada realizada bajo dicha modalidad a través

de la aplicación Chronos, de acuerdo con el apartado 4.3 de la Instrucción 3/2021, de 21 de junio, de esta Dirección General de la Función Pública."

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

HECHOS PROBADOS

1- En la Dirección Provincial de Sanidad de ******LOCALIDAD.1***, (DPS) desde ***FECHA.2 hasta 13/03/2020, en que se suspende por la pandemia, el sistema de control horario empleado ha sido el fichaje mediante comprobación de huella digital. Desde el 13/03/2020, el personal podía fichar a través del ordenador de cada usuario con una aplicación denominada *CHRONOS*. El reclamante que prestaba servicios en dicha sede manifestó que ha estado fichando hasta el 13/03/2020 con ese sistema, aplicable según la reclamada para personal funcionario, eventual o laboral.

2- La Orden de 7/09/2009 de la Consejería de Administraciones Públicas y Justicia sobre horarios de trabajo y vacaciones del personal funcionario regula la duración de la jornada de trabajo, el horario, y la "*necesidad de dotación de medios electrónicos o informáticos adecuados para el control del horario del personal, cumpliendo la normativa vigente sobre protección de datos de carácter personal*."

La Orden 34/2020, de 15/03, de la Consejería de Hacienda y Administraciones Públicas, por la que se regula la prestación de servicios en la Administración General de la Junta de Comunidades de Castilla-La Mancha en desarrollo de las medidas adoptadas como consecuencia de la declaración del estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 estableció como modo habitual de prestación de servicios, la modalidad no presencial, sin perjuicio de que en cualquier momento puedan requerirse modalidades presenciales cuando sea necesario. En desarrollo de la misma, la DG Función Pública adoptó medidas extraordinarias en relación con el control horario del personal de la Admón de la Junta de Comunidades de CLM, resolviendo "*suspender las reglas de control horario previstas en el artículo 13 de la Orden de la Consejería de Admnes. Públicas de 7/09/2009 sobre horarios de trabajo y vacaciones del personal funcionario*

La resolución de la Dirección General de la Función Pública sobre medidas organizativas y de prevención de riesgos laborales para la reincorporación presencial del personal de 10/05/2020 señalaba "*En relación a la utilización de dispositivos de lectura biométrica para el fichaje, se continuará con la medida establecida el 13/03/2020 que posibilita realizar el fichaje mediante CHRONOS a través del ordenador de cada usuario o usuaria*."

3-Según ha manifestado la reclamada, en la DPS de ******LOCALIDAD.1***, desde ***FECHA.2, hasta 13/03/2020, el sistema de control horario empleado ha sido el fichaje mediante comprobación de huella digital, interrumpiéndose por la pandemia y reanudándose el 2/11/2021.

También existe el régimen de teletrabajo (solo puestos de trabajo susceptibles de teletrabajo) que se conjuga con jornadas presenciales-al menos dos a la semana (Instrucción 3/2021 de 29/06 de la DGFP) en el que el registro de la jornada se efectúa a través de la aplicación CHRONOS.

No obstante, en el análisis de riesgos aportado por la reclamada, de 16/01/2021: en cuanto al fichaje, señala que la: "*captura de datos*" para el fichaje, se puede recoger de las siguientes formas,

- *Mediante la lectura de la huella dactilar en el terminal biométrico instalado en las entradas de los edificios. Se recoge la huella, y la fecha y la hora de entrada y salida*.

- *Mediante la introducción de un código facilitado al empleado y que este debe introducir en el terminal biométrico. En este caso, se recoge el código del empleado y la fecha y la hora de entrada y salida.*" La reclamada señala que solo hay un empleado al que se aplica este sistema, que se negó a proporcionar la huella, si bien se informa verbalmente de esta opción a todos, circunstancia que no queda acreditada.

- *A través del ordenador de cada empleado publico en la aplicación FICHAR CHRONOS.*- sin especificar los paréntesis temporales y el colectivo de teletrabajo:

4-Por orden de 5/12/2016, la Consejería de Hacienda y Administraciones Públicas, ejerciendo sus competencias sobre creación, modificación y supresión de ficheros con datos de carácter personal de varias Consejerías de la Junta, determinó la creación del fichero PERSONAL, Diario oficial de CLM de 19/12/2016, "*para la gestión de los RRHH de la Consejería*", en tipos de datos personales que contiene, figura entre otros: "*huella*", en descripción -tipos de datos personales que contiene-, figura: "*Datos relativos a infracciones administrativas*", con la Secretaria General de la Consejería de Sanidad como responsable**.** Manifiesta la reclamada que con la entrada en vigor del RGPD, se transformó en un tratamiento que forma parte del Registro de Actividad del Tratamiento, como "*gestión de personal de la Consejería de Sanidad*", con finalidad: gestión del expediente del personal funcionario, eventual y laboral adscrito a la Consejería, control horario o de presencia del personal, y como base jurídica: la ley 4/2011 de 10/03 del empleo público de Castilla la Mancha, el Real Decreto Legislativo 5/2015 de 30/10 por el que se aprueba la ley del Estatuto básico del empleado público y el Real Decreto Legislativo 2/2015 de 23/10 por el que se aprueba el texto refundido de la de la ley del Estatuto básico de los trabajadores. En Tipos de datos: *"datos relativos a infracciones administrativas, NIF, DNI, número de Seguridad Social, nombre y apellidos, dirección, teléfono, firma, correo electrónico, número de registro de personal, huella. Otros datos: características personales, académicos y profesionales detalles del empleo económicos financieros y de seguros"*

No obstante, la reclamada manifestó que en la base jurídica se basa en los artículos 6.1.b), 6.1.c), 6.1.e) y 9.2.b), del RGPD, y dado que la medida la implantó antes de la entrada en vigor del RGPD, el artículo 6.2 de la LOPD 15/1999.

5-Como ampliación de medidas extraordinarias con el control horario del personal de la Administración de la Junta de Comunidades de Castilla la Mancha, la D. Gral. de la Función Pública resolvió el ***FECHA.3, que el personal, desde el ***FECHA.1 puede emplear el

ordenador del trabajo para realizar el fichaje de manera alternativa al dispositivo de control de huella.

6- Las huellas se almacenan en una base de datos centralizada en SQL Server 11, incluida en la infraestructura certificada. Para la lectura de las huellas se usan terminales de control de acceso con sensores biométricos, marca NITGEN-Fingkey Acces modelo SW101. "*Estos terminales se conectan a un servidor central a través de la red corporativa. La huella se almacena en una base de datos centralizada en SQL Server 11 y se asigna para cada usuario al terminal o terminales desde los que puede fichar, no pudiendo fichar en ningún otro*". La aplicación ACCESS MANAGER hace que la huella se transforme en un código a partir de un algoritmo, y gestiona todas las transacciones de datos entre los terminales y la base de datos centralizada, también la recogida o registro de la huella y codificación, almacenándose en forma cifrada el código de la huella, huella que luego es eliminada.

7- A través de la huella dactilar utilizada por la reclamada, y que sirve con la finalidad de control horario, en entrada y salida del centro de trabajo, la reclamada efectúa deducción de haberes, ajustándose en su calculo a la Ley 1/2021 de 21/02 de medidas complementarias para la aplicación del plan de garantías de servicios sociales de la CCAA de Castilla la Mancha, BOE 13/08/2012. La reclamada efectúa las tareas de control horario utilizando una aplicación denominada *FICHAR CHRONOS,* que también almacena todos los datos en una base de datos tipo SQL Server, y en la que los empleados fichan en el ordenador (RAT), desde el 13/03/2020*,* como consecuencia de la pandemia, al empezar o terminar su jornada laboral, *"sin perjuicio de las especificidades y especialidades de la tipología de personal y servicios públicos a prestar por cada Consejería y Organismo Autónomo*"

8- La reclamada efectuó un análisis de riesgos con fecha **16/01/2021** con la herramienta GESTIONA (que la AEPD pone en la web), a base de una hoja de completar con respuestas 17, dando un resultado de:

-*Riesgos identificados*: Figura un cuadro con "*Amenaza/riesgo*" en el lado izquierdo y en su apartado derecho, "*Riesgo residual*", con el resultado bajo, medio. Destaca:

- *"Manipulación o modificación no autorizada de la información": bajo*

- *"Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información": bajo.*

Finaliza indicando que el resultado obtenido es aceptable, "*por lo que cuando se implanten las recomendaciones realizadas el riesgo sería bajo*".

Se señala como recomendación:

"*Optar por sistemas de verificación o autenticación biométrica 1:1, utilizando la fórmula de combinar código más huella en todos los casos. Además, se recomienda que los sistemas se basen en la lectura de los datos biométricos conservados por la persona trabajadora, por ejemplo en una tarjeta*."

9-Según la reclamada, las garantías adecuadas para la protección de los derechos y libertades de los interesados son las relacionadas con el cumplimiento de los principios de protección de datos recogidos en el artículo 5 del RGPD. En el caso del control horario solo se utiliza para comprobar la presencia del trabajador en su lugar de trabajo durante el tiempo establecido por la Administración. "*Tal y como se ha indicado en el ANEXO 1, en caso de incumplimiento de horario se podrá reducir de la nomina la parte proporcional al tiempo no trabajado*".

10- En un documento diferente, sin fecha ni firma, referido a la idoneidad, necesidad y proporcionalidad alude la reclamada a su uso para evitar suplantar la identidad del empleado, y que se decidió la huella "*tras comprobar el mal uso que se estaba dando a otros sistemas como tarjetas de identificación o códigos*" sin aportar evidencia probatoria.

11-Sobre la Evaluación de Impacto, indica la reclamada que no está obligada a realizarla, pues se trata de un tratamiento que viene de la anterior normativa al RGPD. Indica que "*Dicho tratamiento no ha sufrido ningún cambio tecnológico ni funcional que justifique la realización de esta EIPD*."

12-En pruebas contestó la reclamada que estaba elaborando una evaluación de impacto del control horario.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "*Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos*."

II

Sobre los hechos objeto de reclamación originaria de fecha de 19/08/2020, y su ampliación mediante los escritos de 4 y 8/06/2021, referidos a entregas de documentos sin la debida consideración de la confidencialidad, o reserva, se debe señalar que ya se resolvía y pronunciaba la AEPD sobre estas cuestiones mediante una resolución de inadmisión a trámite que no fue recurrida.

En la ampliación a la reclamación originaria, mediante los escritos de 4 y 8/06/2021, se ponen de manifiesto hechos nuevos. En unos, las pruebas aportadas como la mera presencia de un tercero, empleado, ante la persona que entregaba el documento, sin que se revele un acceso al mismo, o la manifestación de que se entregó el documento en abierto, por un empleado, no son suficientes para entender acreditada la intromisión ilegitima en el derecho de protección de datos, en este caso en el desarrollo de funciones en el empleo público que desarrolla el reclamante. En otros casos, se produce una entrega de documentos de trabajo. Finalmente, datos de contacto como el teléfono, que se contemplan en el tratamiento de gestión de personal, dada la excepcional situación y funciones del puesto a desarrollar. Estas manifestaciones por si solas no constituyen pruebas decisivas para imputar una falta de confidencialidad en el curso del desempeño habitual de las funciones.

III

En cuanto a la reclamación de 8/06/2021, referida al uso de la huella dactilar desde el 13/03/2020, 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;"

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*."

Cada individuo tiene impresiones dactilares únicas que muestran características específicas que pueden medirse para decidir si una impresión dactilar corresponde con una muestra registrada. 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 liberarse de ellos, no se pueden cambiar nunca, ni con la edad, creando cuestiones de responsabilidad en caso de compromiso-pérdida o intrusión en el sistema.

Son datos de cuyo uso pueden desprenderse riesgos significativos para los derechos fundamentales y las libertades, y por ello unos de los denominados de "*categoría especial*", aunque no definidos por el RGPD, en principio está prohibido su tratamiento en el artículo 9.1 del RGPD.

Similar situación de prohibición se contempla en la a Recomendación CM/Reclamante (2015) 5, del Consejo de Ministros del Consejo de Europa a los Estados miembros sobre el tratamiento de datos personales en el contexto laboral. En concreto, el principio 18 de esta Recomendación establece lo siguiente: "*18.1. La recopilación y posterior procesamiento de los datos biométricos solo se deberían emprender cuando hay que proteger los intereses*

legítimos de empresarios, empleados o terceros, solo si no hay otros medios menos intrusivos disponibles y solo si se acompaña de las garantías adecuadas previstas en el principio 21. 18.2. *El tratamiento de los datos biométricos se debe basar en métodos científicamente reconocidos y debe estar sujeto a los requisitos de estricta seguridad y proporcionalida*d".

Una referencia especial a los datos biométricos, se efectúa en el dictamen 4/ 2007 sobre el concepto de datos personales adoptado al 20/06 por el GT 29 (este Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trataba de un organismo de la UE, de carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE), que indica: " *Estos datos pueden definirse como propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad. Ejemplos típicos de datos biométricos son los que proporcionan las huellas dactilares, los modelos retinales, la estructura facial, las voces, pero también la geometría de la mano, las estructuras venosas e incluso determinada habilidad profundamente arraigada u otra característica del comportamiento (como la caligrafía, las pulsaciones, una manera particular de caminar o de hablar, etc.). Una particularidad de los datos biométricos es que se les puede considerar tanto como contenido de la información sobre una determinada persona (Fulano tiene estas huellas dactilares) como un elemento para vincular una información a una determinada persona (este objeto lo ha tocado alguien que tiene estas huellas dactilares y estas huellas dactilares corresponden a Fulano; por lo tanto Fulano ha tocado este objeto). Como tales, pueden servir de «identificadores». En efecto, al corresponder a una única persona, los datos biométricos pueden utilizarse para identificar a esa persona. Este carácter dual también se da en el caso de los datos sobre el ADN, que proporcionan información sobre el cuerpo humano y permiten la identificación inequívoca de una, y sólo una, persona."*

Determina el artículo 9 del RGPD:

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*."

El apartado 2 establece las excepciones que deben concurrir para que el mismo pueda llevarse a cabo, que en materia laboral, con varios condicionantes en su articulado, sería:

"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."

Así pues, en primer termino, para habilitar el tratamiento de los datos biométricos, debe cumplir alguno de los supuestos específicos de habilitación de ese tipo de tratamiento conformado por el régimen del artículo 9. 2, letras a) a j), siendo el mas próximo al ámbito laboral el de la letra 9.2.b) y además de darse la circunstancia que levante en su caso la prohibición de tratamiento, debe concurrir alguna de las bases legitimas para que el tratamiento de datos sea lícito, que se definen en el artículo 6.1 del RGPD, y cumplir con los principios que se expresan en el artículo 5 del RGPD, entre los que juegan importante papel la minimización y proporcionalidad y necesidad de tratamiento de esos datos.

El artículo 6.1 del RGPD señala:

"*1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."

El artículo 7 de la Carta de Derechos Fundamentales de la Unión Europea, proclamada por el Parlamento Europeo y el Consejo de la Unión Europea y la Comisión de 7/12/2000, prescribe que toda persona tiene derecho al respeto a su vida privada, y el artículo 8.1, que toda

persona tiene derecho a la protección de datos de carácter personal que le conciernen. Interpretadas conjuntamente, se infiere que puede constituir una vulneración de tales derechos cualquier tratamiento de datos, en este caso la reclamada. Esta utilización de los datos de como empleados de la reclamada, con los medios y fines decididos por la misma, bajo sus condiciones, supone una intromisión de su derecho a la vida privada y a la protección de datos si no resultara justificada. El artículo 8.2 de la Carta de Derechos fundamentales precisa que los datos de carácter personal solo pueden ser tratados con el consentimiento del interesado o en virtud de otro fundamento legitimo previsto por Ley. Además, los artículos 7 y 8 de la Carta no son absolutos, admitiendo limitaciones, siempre que estén previstas por la Ley, respeten el contenido esencial de esos derechos y con observancia del principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás (Sentencia del Tribunal de Justicia de la Unión Europea, sala cuarta, sentencia de 15 /10/2013, C/291/2012.). Estos aspectos por lo demás, se reiteran en relación con los derechos fundamentales, en el art. 52.1 *in fine* de la Carta de los Derechos Fundamentales de la UE.

El análisis de la legitimidad del tratamiento biométrico ha de estar basado en una base legitimadora, pero también si el tratamiento es necesario, proporcional y se puede llevar a cabo con un riesgo bajo para los derechos y libertades de los interesados.

En este caso, se refiere al tratamiento de datos a través del sistema de registro de huellas para el cumplimiento del registro de control horario, control este, que se establece como obligación en el ámbito de la administración reclamada por la Orden de 07/09/2009, de la Consejería de Administraciones Públicas y Justicia, sobre horarios de trabajo y vacaciones del personal funcionario. Esta Orden, como disposición administrativa, complementa "el Acuerdo entre la Administración de la Junta de Comunidades de Castilla-La Mancha y las organizaciones s*indicales, por el que se establece el Plan para la conciliación de la vida familiar y laboral de las empleadas y empleados públicos de la Administración de la Junta de Comunidades de Castilla-La Mancha*" que prevé en su apartado 5, la adaptación y modificación de las normas reguladoras del régimen de horarios de trabajo de los distintos sectores del empleo público, al objeto de incorporar criterios de racionalización y flexibilización de la jornada de trabajo que permitan compatibilizar del mejor modo posible la jornada diaria de trabajo con la vida familiar, sin merma en la adecuada prestación de los servicios públicos. La Orden establece para los centros y oficinas de la Administración de la Junta de Comunidades de Castilla-La Mancha y de sus organismos públicos: "*dotarse de los medios electrónicos o informáticos adecuados para el control del horario del personal".* No señala ni impone el instrumento o sistema concreto a utilizar, y no se discute la necesidad de hacer este tipo de control, sino de hacerlo a través de la técnica propuesta, esto es, el uso de sistemas de identificación basados en datos biométricos y la determinación de la necesidad y proporcionalidad del mismo.

En cuanto al propio objeto de la reclamación, la manifestación del reclamante sobre que no se solicitó por la reclamada el consentimiento para el sistema de la toma y uso de la huella dactilar como registro de jornada laboral, se indica que el consentimiento es solo una de las causas que habilitaría el tratamiento de esos datos, si bien "*es muy poco probable que el consentimiento constituya una base jurídica para el tratamiento de datos en el trabajo, a no ser que los trabajadores puedan negarse sin consecuencias adversas* […] (dictamen 2//017 sobre el tratamiento de datos en el trabajo, del Grupo de Trabajo del artículo 29).

Sobre la manifestación de la reclamada de que su sistema de control horario se ajustaba en cuanto a base legitimadora, a lo dispuesto en el artículo 6.2 de la LOPD 15/1999;

"2*. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento*"

Debe partir de la base de que dicha LOPD, es desarrollo de la Directiva 95/46, del Parlamento Europeo y del Consejo de 24/10/1995, 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, que establecía en su artículo 7 los principios relativos a la legitimación del tratamiento de datos, en similar redacción al artículo 6 del RGPD, indicando aquella:

"Los Estados miembros dispondrán que el tratamiento de datos personales solo puede efectuarse si:

a) el interesado ha dado su consentimiento de forma inequívoca, o

b) es necesario para la ejecución de un contrato en el que interesado sea partido para la aplicación de medidas precontractuales adoptadas a petición del interesado, o

c) es necesaria para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento ,o

c) es necesario para proteger el interés vital del interesado, o

d) es necesaria para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento a un tercero a quien se comuniquen los datos, o

e) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva."

Las competencias relacionadas con el control horario no se desarrollan de forma que determinen los medios instrumentales para llevarlos a cabo, incidiendo en un derecho fundamental de sus titulares, por lo que cualquier injerencia en los mismos ha de estar prevista expresamente en una Ley. En este caso, la determinación de ejercicio de competencias es un termino inespecífico que no supone per se sino tan solo el fin, no los medios. Asimismo, la Ley que contuviera dicha mención, debería establecer las garantías para el tratamiento de los derechos de las personas. Por lo demás, siendo preciso el control horario, el mantenimiento o cumplimiento del mismo no depende de la instauración y uso de la huella dactilar, elemento físico corporal titularidad del empleado único, sobre el que se impone la obligación de uso, imponiendo su colaboración para ser recogido y usado, como obligatorio, sin norma legal que expresamente lo imponga.

El sistema de registro de jornada para el control horario a través de la huella dactilar puede tener ventajas, pero no es el único que permite garantizarlo. Habría que cuestionar si es ne-

cesario el tratamiento en relación con el fin que se persigue y la proporcionalidad objetiva del tratamiento, ya que 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 sea necesaria, ello constituye per se una limitación del derecho de protección de datos.

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.

A tal efecto y como ejemplo, ya el 10/10/2017, el EDPS-Supervisor Europeo de Protección de Datos, autoridad supervisora independiente que tiene como objetivo principal garantizar que las instituciones y órganos de la Unión Europea respeten el derecho a la intimidad y la protección de datos cuando tratan datos de carácter personal- no consideró proporcionado el uso del sistema biométrico de la huella para el control de personal de trabajo y salida del personal en el Parlamento Europeo, al no considerarlo necesario ni proporcional en relación con la finalidad, que podía ser conseguida con medios menos intrusivos (https://edps.europa.eu/sites/edp/files/publication/20-10-07_edps_biometrics_speech_en.pdf), y https://edps.europa.eu/data-protection/our-work/publications/supervisory-opinions/use-computerised-system-european_en.

En cuanto al control presencial que se efectúa con la huella dactilar, las personas que teletrabajan pueden en esas jornadas fichar mediante el ordenador, y en el periodo de pandemia estuvo vigente ese sistema, sustituyendo temporalmente a la huella digital. Sin embargo, se ha retomado el uso de la huella. Con todo, no que da clara la explicación de que a una persona se le posibilite el uso de códigos numéricos sin huella, porque se negó a darla, al mismo tiempo que explica que ese modo existe por si falla la huella. Con ello, se desvela que se produce una diferenciación de trato sin fundamento que no consta se ofreciera al resto de empleados, y que es factible al menos otro medio de control a la huella, sin perjuicio de que la reclamada tampoco respondiera a la opción que resultó de los riesgos que señalaba:

"*Optar por sistemas de verificación o autenticación biométrica 1:1, utilizando la fórmula de combinar código más huella en todos los casos. Además, se recomienda que los sistemas se basen en la lectura de los datos biométricos conservados por la persona trabajadora, por ejemplo en una tarjeta*."

Una alternativa al uso no es una medida pensada para cuando falla la prevista sino que debe ser, de inicio, una doble opción. Un empleado usa un código porque se negó al registro y uso de la huella, facilitándose la medida que a la vez se dio al resto de empleados verbalmente, hecho que no puede acreditar que se hubiera dado a los demás empleados, dado que el deber de documentar las decisiones en cuestiones de tratamiento de datos han de ser documentadas, y verbalmente es una mera manifestación que ni tiene porque haberse producido, ni que se haya dado a todos los empleados, y en todo caso, de difícil prueba.

IV

Conforme al RGPD artículo 5, apartado 1, letra a), además de la obligación de que los datos se traten de manera lícita y leal, la transparencia se incluye como aspecto fundamental de estos principios.

La transparencia está intrínsecamente ligada a la lealtad y al nuevo principio de responsabilidad proactiva del RGPD. Asimismo, del artículo 5, apartado 2, también se desprende que los responsables del tratamiento siempre deben estar en condiciones de demostrar que los datos personales se tratan de manera transparente en relación con el interesado. El principio de responsabilidad requiere que el responsable asuma la responsabilidad de lo que hace con los datos personales y cómo cumple con los demás principios, y debe contar con medidas y registros apropiados para poder demostrar su cumplimiento.

Conforme al considerando 171 del RGPD, "*todo tratamiento ya iniciado en la fecha de aplicación del presente reglamento debe ajustarse al presente reglamento en el plazo de dos años a partir de la fecha de su entrada en vigo*r" y los responsables del tratamiento deben velar por que este sea conforme con sus obligaciones de transparencia a partir del 25/05/2018 (además de con el resto de las obligaciones en virtud del RGPD). Esto implica que, antes del 25/05/2018, los responsables del tratamiento de datos deberían revisar toda la información facilitada a los interesados sobre el tratamiento de sus datos personales para garantizar que cumplen los requisitos de transparencia. Cuando se introduzcan cambios o adiciones en dicha información, los responsables del tratamiento deben dejar claro a los interesados que estos cambios se han realizado para cumplir con el RGPD. El GT29 recomienda que estos cambios o adiciones se pongan activamente en conocimiento de los interesados, pero, como mínimo, los responsables del tratamiento deben poner esta información a disposición del público (p. ej., en su sitio web). No obstante, si los cambios o adiciones son importantes o sustanciales, estos cambios deben ponerse activamente en conocimiento del interesado.

Cuando los responsables del tratamiento actúan con transparencia, esta capacita a los interesados para pedir cuentas a los responsables y los encargados del tratamiento y para ejercer el control sobre sus datos personales.

Los requisitos de transparencia contenidos en el RGPD se aplican independientemente de la base jurídica para el tratamiento y a lo largo de todo el ciclo de vida del mismo. Esto queda patente en el artículo 12, que prevé que la transparencia se aplique en las siguientes etapas del ciclo del tratamiento de datos:

• antes del ciclo del tratamiento de datos o al inicio del mismo, es decir, cuando se recogen los datos personales a través del interesado o por otros medios;

• a lo largo de todo el periodo de tratamiento, es decir, cuando se comunican a los interesados sus derechos; y

• en momentos específicos mientras el tratamiento está en curso, por ejemplo, cuando se producen violaciones de la seguridad de los datos o en caso de que se produzcan cambios importantes

Además de los cambios en las obligaciones de transparencia, los principios de lealtad y responsabilidad proactiva inciden en los derechos de los titulares de los datos con la aplicación y entrada en vigor del RGPD. La nueva categorización de los datos biométricos en datos especiales y su prohibición inicial de tratamiento, supone no solo que se debió implementar la comunicación de los nuevos elementos de transparencia en el tratamiento llevado a cabo

desde 2016 a las aspectos sustanciales implicados con la modificación en la política de privacidad del tratamiento de la huella, categoría especial que como riesgos específicos que conlleva su tratamiento, ha de contar con unas salvaguardas diferenciadas de otras categorías de datos. Con tal previsión, no se puede indicar que no existe seguridad jurídica en la previsión que de la prohibición con anticipación considerable que estableció el RGPD. Sin que se prejuzgue que el hecho de que en un momento inicial se implantase un sistema no pueda implicar que se actualice a lo exigido como obligatorio con un cambio en la normativa, a la que se ha tenido tiempo para adaptarse.

V

El RGPD hace depender la aplicación de todas las medidas de cumplimiento que prevé para responsables y encargados, del nivel y tipo de riesgo que cada tratamiento implique para los derechos y libertades de los afectados. El artículo 28 de la LOPDGDD, señala como obligaciones:

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

El articulo 32 del RGPD también señala como uno de los factores a tener en cuenta, "*los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas" para la aplicación de medidas apropiadas para garantizar* "*un nivel de seguridad adecuado al riesgo*".

Del cambio de paradigma con la normativa anterior operado con el RGPD, es prueba el hecho de que la exigencia de que las medidas de seguridad se han de adecuar a las características de los tratamientos, sus riesgos, y el contexto y tecnología en que se desarrolla el estado de la técnica y los costes. Ello contrastaría con la LOPD anterior al RGPD, que basaba las medidas de seguridad atendiendo básicamente al tipo de datos que se tratasen. La aplicación ahora de las medidas no puede derivarse automáticamente de que se traten unos u otros datos, sino que ha de ser la consecuencia de un análisis de riesgos específico para cada tratamiento.

La gestión de riesgos relacionados con las operaciones de tratamiento de datos sujetas al RGPD implica que todas las decisiones relacionadas con dicho tratamiento, y no sólo las vinculadas a la seguridad de los mismos, se han de sustentar en la gestión de los riesgos. Siempre hay un riesgo inherente al tratamiento, por el hecho mismo de llevarlo a cabo, por ello lo que persigue el proceso de gestión de riesgos es mantenerlos identificados, evaluados y tratarlos, estableciendo una respuesta a éstos, adoptando las salvaguardas necesarias para reducir dichos riesgos hasta un nivel considerado aceptable.

En el contexto de las AA.PP. , aparte de las metodologías de análisis de riesgos focalizadas en la seguridad de la información, se han de ampliar para incluir riesgos asociados al incumplimiento de las disposiciones del RGPD, en tanto que son responsables del tratamiento de los datos de los ciudadanos, o de sus empleados. Antes de poner en marcha nuevas actividades de tratamiento o modificar servicios ya prestados que hagan uso de nuevas tecnolo-

gías, deberán identificar aquellos riesgos a los que pueda estar expuesto el tratamiento. Por ello, todo tratamiento, tanto los ya existentes como los que se pretenda iniciar, deben ser objeto de un análisis de riesgos. Riesgos que no son estáticos, evolucionan de forma continua, por lo que una vez identificado, exige un esfuerzo de supervisión permanente. La actitud correcta es conocer el riesgo, evaluar sus consecuencias, tomar medidas para minimizarlo y controlar su efectividad en un contexto cambiante. Este esquema de supervisión continua es lo que se define como la gestión del riesgo.

El riesgo debe determinarse basándose en una evaluación objetiva, mediante la cual se determine si las operaciones de tratamiento de datos suponen un alto riesgo. Un alto riesgo es un especial riesgo de perjuicio para los derechos y libertades de los interesados.

La evaluación, gestión y minimización del riesgo para los derechos y libertades es una obligación del responsable del tratamiento (artículos 23.2.g, 24.1, 25, 32, 33, 34, 35 y 36 entre otros del RGPD) y forma parte de la lista de cumplimiento normativo. El RGPD, aunque da algunas indicaciones, no es concreto a la hora de identificar y pautar cómo realizar la gestión del riesgo de cada tratamiento de forma específica.

La reclamada aporta copia de las "*medidas de seguridad que garantizan que los datos personales presentan los mínimos riesgos de seguridad, según el análisis de riesgos realizado*" que acompañan como ANEXO IV, realizado el 16/01/2021, con la herramienta GESTIONA de la AEPD. Sobre esta valoración, se debe concretar:

-Es una herramienta de ayuda al cumplimiento normativo que pretende dar soporte a la decisión y cuya utilización genera la documentación básica, en ningún caso exhaustiva sobre la que hay que realizar un análisis y gestión de riesgo por parte de los responsables de cumplir con lo previsto en el RGPD y LOPDGDD. Está documentación básica será un punto de partida que debe ser completado siguiendo las indicaciones de gestión de riesgo y evaluación de impacto en tratamiento de datos personales.

-Es una herramienta orientada a PYMES, no a Administraciones Públicas, que son sujetos distintos, con perfiles de riesgos distintos en el tratamiento con el añadido de que puede imponer los tratamientos a todo un amplio colectivo, con la imposibilidad en muchos casos de oponerse, afectando derechos y libertades, como podría ser entre otros: reducción proporcional de haberes como tiempo de servicio no trabajado o no justificado a través del sistema de registro de jornada con la huella dactilar implantado antes de la entrada en vigor del RGPD, con la LOPD, y que por tanto puede producir efectos en los derechos de los empleados.

La Guía para una Evaluación de Impacto en la Protección Datos Personales» que publicó en 2014 la AEPD, indicaba que existen múltiples metodologías de análisis de riesgos y pueden resultar adecuadas para el objetivo buscado, sin incluir directrices específicas en ese ámbito. Pero por su relevancia y adaptación al caso específico de la privacidad, se hizo mención a la publicación "*Methodology for Privacy Risk Management*" de la Commission Nationale de l'Informatique et des Libertés (CNIL), a *MAGERIT* (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), herramienta creada por el Consejo Superior de Administración Electrónica para asistir a los distintos organismos públicos en este ámbito, a Risk IT (ISACA) o ISO 27005, y destacando también a estos efectos la utilidad de las normas ISO 31000 sobre principios y directrices de gestión del riesgo y la norma ISO 31010 sobre técnicas de gestión de riesgos, en la que se detallan diversos métodos que pueden ayudar a identificar y detectar los riesgos de un nuevo producto o servicio.

-Lo que aporta la reclamada de las medidas de seguridad del tratamiento referidas a los riesgos, no tiene en cuenta el hecho de que los riesgos a valorar en relación con la seguridad son solo uno de los aspectos a cubrir, ignorando la gestión de los riesgos de los derechos y libertades en el ámbito del tratamiento de datos personales, así como la eficacia y la efectividad de las garantías jurídicas y técnicas aplicadas.

-No ha valorado opciones menos intrusivas como al que se incluía de:

"*Optar por sistemas de verificación o autenticación biométrica 1:1, utilizando la fórmula de combinar código más huella en todos los casos. Además, se recomienda que los sistemas se basen en la lectura de los datos biométricos conservados por la persona trabajadora, por ejemplo en una tarjeta*."

VI

Se deduce del análisis llevado a cabo hasta el momento, que se están tratando datos de carácter personal de categoría especial, así considerados por el RGPD.

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

La evaluación de impacto en la protección de datos personales, EIPD, es la herramienta que en el RGPD se ocupa de la garantía de cumplimiento de esta vertiente del tratamiento.

En el texto del RGPD no aparece una definición para el término "evaluación de impacto relativa a la protección de datos" o EIPD. El Grupo de Trabajo 29, GT 29, creado de conformidad con el artículo 29 de la Directiva 95/46/CE, órgano consultivo independiente de la UE en materia de protección de datos y privacidad con funciones descritas en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE. desarrolla la definición de EIPD en las Directrices WP248 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 el 4/04/2017 y revisadas por ultima vez y adoptadas el 4/10/2017, como: "… *un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos*." Según esto, el la EIPD, es un "*proceso*" y, por tanto:

• Reducir la EIPD a una actividad puntual y aislada en el tiempo es incompatible con el concepto de proceso que interpreta las Directrices WP248.

• La EIPD ha de estar documentada, pero la EIPD es más que el informe que refleja sus resultados.

• La EIPD ha de evaluar los riesgos "*determinando las medidas para abordarlos*". La EIPD obliga al responsable a actuar y tiene una dimensión mayor que un mero formalismo plas-

mado en un documento sobre el que se puedan realizar cambios mínimos para adaptarlo a cualquier tratamiento.

La EIPD es un proceso de análisis de un tratamiento que se extiende en el tiempo, a lo largo de todo el ciclo de vida de un tratamiento de datos personales, y que se ha de revisar de forma continua, "*al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento*" (art.35.11 del RGPD).

El RGPD impone la obligación de disponer de una Evaluación de Impacto en la Protección de los Datos Personales (EIPD), determinando su 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 no exhaustiva 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 establecidos por las "*DIRECTRICES SOBRE LA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD) Y PARA DETERMINAR SI EL TRATAMIENTO «ENTRAÑA PROBABLEMENTE UN ALTO RIESGO»*

A EFECTOS DEL RGPD", adoptadas el 4/04/2017 y revisadas por ultima vez y adoptadas el 4/10/2017, WP 248 rev.01 del GT 29 que los complementa y debe entenderse como una lista no exhaustiva:

La lista señala:

"*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…"

En las Directrices, se señala:

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

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

La reclamada acude para la instauración del sistema de control horario a datos biométricos que forman parte de la identidad física, que no cambia con el transcurso del tiempo, y que precisa por parte de su titular, el empleado, de una colaboración activa para inscribir sus datos y acceder cada vez que acuda al centro de trabajo colocando el dedo en el terminal de lectura, permitiendo que partes de sus órganos se sometan a las operaciones necesarias para el funcionamiento del sistema. Asimismo, puede sufrir repercusiones en sus derechos al condicionarse decisiones automatizadas producto del uso del sistema de control que pueden afectar al empleado, por el control de las deducciones de haberes.

El RGPD no requiere que se realice una EIPD para cada operación de tratamiento que pueda entrañar riesgos para los derechos y libertades de las personas físicas. La realización de una EIPD es únicamente obligatoria cuando el tratamiento "*entrañe probablemente un alto riesgo para los derechos y libertades de las personas física*s". Es posible que las actividades ordinarias de control horario no entrañen probablemente un alto riesgo para los derechos y libertades de los interesados, pero si se introducen nuevas tecnologías y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resulta necesaria visto el tiempo transcurrido desde el tratamiento inicial debe

establecerse esta obligación (considerando 89 del RGPD).

"*En tales casos, el responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento*". (considerando 90).

"*La evaluación de impacto relativa a la protección de datos debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas.*"(considerando 91).

El RGPD establece la obligación de gestionar el riesgo que para los derechos y libertades de las personas supone esos tratamientos. Este riesgo surge tanto por la propia existencia del tratamiento, como por las dimensiones técnicas y organizativas del mismo. El riesgo surge por los fines del tratamiento y su naturaleza, y también por su alcance y el contexto en el que se desenvuelve, y precisa que que los responsables del tratamiento apliquen medidas adecuadas para garantizar y poder demostrar el cumplimiento de dicho reglamento, teniendo en cuenta entre otros «*los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas*» (artículo 24, apartado 1). Estos derechos y libertades de los interesados atañen principalmente a los derechos de protección de datos y a la intimidad, pero también pueden implicar otros derechos fundamentales como por ejemplo la prohibición de discriminación, la libertad de circulación, etc. .La obligación de los responsables del tratamiento de llevar a cabo una EIPD en determinadas circunstancias debe entenderse en el contexto de su obligación general de gestionar adecuadamente los riesgos derivados del tratamiento de datos personales.

La complejidad del proceso de gestión de riesgo ha de ajustarse, no al tamaño de la entidad, la disponibilidad de recursos, la especialidad o sector de la misma, sino al posible impacto de la actividad de tratamiento sobre los interesados y a la propia dificultad del tratamiento.

El tratamiento biométrico presenta entre otros los siguientes riesgos, algunos de los cuales se contemplan en el DICTAMEN 3/2012 SOBRE LA EVOLUCION DE LAS TECNOLOGÍAS BIOMETRICAS del GT 29 de 27/04/2012:

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

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

- No hace falta decir que toda pérdida de las cualidades de integridad, confidencialidad y disponibilidad con respecto a las bases de datos sería claramente perjudicial para cualquier aplicación futura basada en la información contenida en dichas bases de datos, y causaría asimismo un daño irreparable a los interesados. Por ejemplo, si 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. El resultado sería 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. La realidad de la tecnología es que cada día nuevas formas de ingeniería social generan nuevas vulnerabilidades que aparecen en el marco del tratamiento donde las operaciones biométricas se sitúan, por lo que es necesario considerar escenarios de brechas de datos y determinar el impacto que una brecha de datos hola e podría causar en los derechos y las libertades de los interesados. Asimismo, es necesario conocer la realidad de qué incumplimientos ya se están produciendo y cuáles podrían determinar la inadecuación de la técnica biométrica o de la biometría en general. Esto implica una evaluación continua del tratamiento en función de los hechos que se vayan produciendo.

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

-Se puede crear la ilusión de que la identificación a través de la huella siempre es correcta, por ello se debe incluir un análisis de los errores que se pueden producir en su uso, medidores de evaluación del rendimiento, tasa de falsa aceptación- probabilidad de que un sistema biométrico identifique incorrectamente a un individuo o no rechace a un individuo que no pertenece al grupo, y tasa de falso rechazo o falso negativo: no se establece la correspondencia entre una persona y su propia plantilla. Todo ello con los efectos de poder constituirse como prueba plena en lo que respecta a la acreditación de la presencia de una persona determinada en el lugar en que se encuentre, con la relación de las decisiones que afecten jurídicamente a una persona , decisión que debería efectuarse salvaguardando los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

-Deben adoptarse medidas de seguridad con motivo del tratamiento de datos biométricos (almacenamiento, transmisión, extracción de características y comparación, etc.) y sobre todo si el responsable del tratamiento transmite esos datos a través de Internet. Las medidas de seguridad podrían incluir, por ejemplo, la codificación de las plantillas y la protección de las claves de codificación aparte del control del acceso y una protección que convierta en virtualmente imposible la reconstrucción de los datos originales a partir de las plantillas.

-Asimismo, el DOCUMENTO DE TRABAJO SOBRE BIOMETRÍA, adoptado el 1/08/2003, del GT29, opina que los sistemas biométricos relativos a características físicas que no dejan rastro (por ejemplo la forma de la mano, pero no las huellas digitales) o los sistemas biométricos relativos a características físicas que dejan rastro pero no dependen de la memorización de los datos poseídos por una persona distinta del interesado (en otras palabras, los datos no se memorizan en el dispositivo de control de acceso ni en una base de datos central) crean menos riesgos para la protección de los derechos y libertades fundamentales de las personas (Se pueden distinguir los datos biométricos que se tratan de manera centralizada de los datos de referencia biométricos que se almacenan en un

dispositivo móvil y el proceso de conformidad se realiza en la tarjeta y no en el sensor o cuando éste forma parte del dispositivo móvil).

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

- Riesgos evidentes si la tecnología empleada no garantiza de manera suficiente que la plantilla obtenida a partir de los datos biométricos no coincidirá con la empleada en otros sistemas similares.

Todo ello, sin perder de vista que se trata de un sistema de identificación muy intrusivo para los derechos y libertades fundamentales de las personas físicas, entre otras circunstancias por el funcionamiento a través de sistemas de inteligencia artificial que implementan algoritmos para diseñar y leer la plantilla biométrica, puesto en relación con la deficiencia en las normas de fabricación de sistemas homologados y certificados del software de uso, añadido a la extensión e interoperabilidad de uso de estos sistemas.

Todos estos elementos contribuyen a considerar como probable el alto riesgo para los derechos y libertades de las personas físicas que se mencionan en el artículo 35.1 del RGPD, al que además se refieren en este caso dos condiciones del listado de la AEPD del artículo 35.4 del RGPD.

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

En cuanto a la manifestación de la reclamada de que no se efectuó la EIPD porque el sistema de huella dactilar tratando los datos personales con la finalidad de registro de jornada laboral se instaura el ***FECHA.2, bajo la vigencia de la LOPD y no ha sufrido ningún cambio tecnológico ni funcional que justifique la realización de esta EIPD, se debe añadir que las Directrices del GT 29 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 Reglamento (UE) 2016/679 adoptadas el 4/04/2017, revisadas por última vez y adoptadas el 4/10/2017, indican sobre las operaciones de tratamiento ya existentes que "*El requisito de realizar una EIPD se aplica a operaciones de tratamiento existentes que probablemente entrañan un alto riesgo para los derechos y libertades de las personas físicas y para las que se ha producido un cambio de los riesgos, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento*"

Además del fundamento de derecho precedente que pone de manifiesto que se ha ejecutado una valoración básica insuficiente y no adecuada de riesgos para los derechos y liberta-

des de los afectados, se debe de añadir que además, dentro del contexto, hay que tener en cuenta que cuando se puso en funcionamiento, septiembre 2016, ya estaba publicado varios meses antes en el DOUE el 4/05/2016, el RGPD, que tenia dispuesta su entrada en vigor el 24/05/2016, aplicable a partir del 25/05/2018, por lo que la prohibición del uso de datos biométricos como regla general era conocida desde antes no ya de su puesta en marcha, sino de la publicación en diciembre 2016 del fichero PERSONAL en el que se encontraba el uso de la huella.

En cuando a la consideración de datos biométricos como datos especiales, hay que tener en cuenta que en las propuestas sobre el paquete de reforma de la Protección de Datos, que desembocó en la aprobación el RGPD, la Comisión Europea, solo añadió a la lista de datos sensibles, los datos genéticos. Fue el Parlamento Europeo quien añadió a la lista de datos sensibles, los biométricos, cuando votó la propuesta del RGPD el 14/03/2014, a pesar de que algunas autoridades nacionales sugirieron por su naturaleza especifica añadirlos a la lista de datos sensibles. Ello acredita que se ha producido un cambio de contexto con la aprobación de dicha normativa que afecta especialmente a los datos biométricos que pasaron de datos genéricos a la categoría de datos especiales como aspecto novedoso en dicha normativa de aplicación europea, variando no solo los medios tecnológicos desde la eventual implantación del sistema por la reclamada, sino los riesgos, y su extensión en ámbitos de clara afectación al ejercicio de derechos fundamentales, con la consideración que como tal protección merece.

Asimismo, la implantación del sistema por la reclamada en su día, no tiene porque significar sin mas que ha sido legitimado mientras se ha estado usando, sin haber tenido oportunidad de pronunciarse la autoridad supervisora sobre si cumple los elementos que tiene que completar este tipo de tratamientos.

Una EIPD debe percibirse como un instrumento de ayuda en la toma de decisiones relativas al tratamiento, por lo que es recomendable realizarla en las fases de concepción y diseño del tratamiento. Con ello se cumpliría con los principios de protección de datos desde el diseño, y ayuda a que las garantías seleccionadas estén guiadas por la gestión del riesgo y se implementen durante la fase de concepción y diseño del tratamiento, estando integradas en el mismo y extendiéndose a todas las etapas de su ciclo de vida. La protección de datos desde el diseño no es una capa adicional o un elemento que se puede añadir a posteriori. Por lo tanto, una EIPD, puede implicar que hay que realizar cambios en el tratamiento para introducir modificaciones, garantías o medidas para reducir los riesgos, se ha de realizar antes y durante la fase de diseño, y el enfoque de riesgos que supone la EIPD es un proceso, no un estado.

La reclamada no contempló los diversos y variados elementos que se han señalado en este apartado en su valoración de riesgos, y ha manifestado que no existe riesgo o este es aceptable, debiendo estos elementos formar parte de la citada evaluación de impacto.

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. La reclamada no acredita haber cumplido con esta obligación, estimando que puede haber incurrido en la citada infracción del artículo 35 del RGPD.

VII

La infracción imputada se tipifica en al artículo 83.4.a) del RGPD que indica:

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

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

La LOPDGDD establece a efectos de prescripción de la infracción, 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:*

"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;"

f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;
[…]"

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;"

"*La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD*."

La reclamada continúa utilizando la huella dactilar sin haber realizado una evaluación de impacto sobre esa operación de tratamiento que entraña probablemente un alto riesgo en los derechos y libertades de los empleados. Así pues, entre otras cuestiones, continúan sin identificar los riesgos asociados al tratamiento del uso de la huella dactilar para control horario, y por tanto sin poder mitigarlos, existiendo otras modalidades que para dicho fin tiene instaurada la reclamada. Se considera pues, con el fin de garantizar los derechos y

libertades de los titulares de los datos, que concurre la necesidad y justificación de adoptar poderes correctivos que se determina en la parte dispositiva.

El artículo 90.3 de la LPCAP indica que "*la resolución que ponga fin al procedimiento será ejecutiva cuando no quepa contra ella ningún recurso ordinario en vía administrativa, pudiendo adoptarse en la misma las disposiciones cautelares precisas para garantizar su eficacia en tanto no sea ejecutiva*"

Considerando que la reclamada es una entidad publica que forma parte de la CCAA de Castilla La Mancha, el artículo 83.7 del RGPD señala:

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

El "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone en su artículo 77:

[…]"

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.
(…)
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."

En su apartado 1 señala

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

[…]"

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local. "

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: SANCIONAR a **CONSEJERÍA DE SANIDAD DE LA JUNTA DE COMUNIDADES DE CASTILLA-LA MANCHA**, con NIF ***S1911001D***, con apercibimiento por una infracción del artículo 35 del RGPD, de conformidad con el artículo 83.4 a) del RGPD, y a efectos de prescripción de la infracción en el artículo 73.t) de la LOPDGDD.

SEGUNDO: Requerir en aplicación de los artículos 90.3 de la LPCAP, y 58. 2.f), del RGPD, a la **CONSEJERÍA DE SANIDAD DE LA JUNTA DE COMUNIDADES DE CASTILLA-LA MANCHA**, para que en el plazo de diez días, "limite *temporal o definitivamente el tratamiento"* del sistema de control horario mediante la huella dactilar, en tanto no disponga de una evaluación de impacto de protección de datos del tratamiento válida, que tenga en cuenta los riesgos para los derechos y libertades de los empleados y las medidas y garantías adecuadas para su tratamiento, o incluso si se realizara, precisara efectuar la previsión de consulta que se establece en el artículo 36 del RGPD.

Transcurrido el tiempo otorgado, deberá informar a esta AEPD.

La falta de atención al requerimiento puede dar lugar a la comisión de una infracción del artículo 83.6 del RGPD,

TERCERO: NOTIFICAR la presente resolución a **CONSEJERÍA DE SANIDAD DE LA JUNTA DE COMUNIDADES DE CASTILLA-LA MANCHA**.

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

QUINTO: 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 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.

938-181022

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