- **Expediente N.º: EXP202213615**

Procedimiento Sancionador N.º PS/00074/2024

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas 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 10 de noviembre de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra ***AYUNTAMIENTO DE TELDE*** con NIF ***P3502600D*** (en adelante, la parte reclamada/ el Ayuntamiento).

La parte reclamante solicita que analice la legalidad de la imposición del fichaje mediante el reconocimiento facial que se establece como método de control de la jornada laboral para los empleados municipales del Ayuntamiento, revisando si se ha efectuado una evaluación de impacto previa al tratamiento de los datos biométricos y que se le comunique si la parte reclamada ha cumplido la obligación de designar un delegado de protección de datos.

Los motivos en que basa la reclamación son los siguientes:

- El 19/01/2022 la parte reclamante, empleado de la policía municipal del Ayuntamiento de Telde, presentó un escrito ante el registro del Ayuntamiento, en el que solicitaba que:

  " *Que se le reconozca el derecho a fichar electrónicamente a través del móvil con geolocalización y en consecuencia, la Concejalía de Recursos Humanos facilite al solicitante los medios técnicos necesarios para fichar a través de este procedimiento por ser proporcional a la finalidad perseguida, toda vez que es menos invasivo en materia del derecho fundamental a la protección de datos que el procedimiento alternativo de reconocimiento facial; y en igualdad de condiciones que otros empleados municipales*".

  Manifiesta el reclamante que tal solicitud se basa en la Circular de 10/01/21 emitida por la Concejalía de Economía y Recursos Humanos del Ayuntamiento, y el posterior Reglamento del Pleno del Ayuntamiento, que establecían 3 posibles vías de fichaje de la jornada laboral: fichaje el reconocimiento facial, el fichaje a través de la web, y el fichaje a través del móvil con geolocalización.

  También indica que tal solicitud se formuló primeramente por correo electrónico a la Concejalía de Recursos Humanos, siéndole denegada el 11/1/21, por estar reservado este tipo de fichaje a servicios determinados, e indicándole que en su caso debía fichar por el sistema de reconocimiento facial en el terminal que consta en las instalaciones de la policía municipal.

- La petición formulada el 10/01/21 fue denegada por el Ayuntamiento por resolución de 26/01/22 por no ser el sistema de fichaje de elección del empleado

sino parte de la potestad organizativa del Ayuntamiento, lo que fue recurrido por la parte reclamante mediante recurso de reposición, que fue desestimado por el mismo motivo el 28/04/22.

- El 04/05/22 la parte reclamante solicita al Ayuntamiento que se le asigne lugar, fecha y hora para la toma de los datos biométricos. E incluye una petición para que el delegado de protección de datos (en adelante, DPD) supervise el cumplimiento de la normativa de protección de datos y determine: si se ha efectuado una evaluación de impacto previa al tratamiento de los datos biométricos, que se pronunciase sobre la obligación de realizar el fichaje mediante reconocimiento facial en lugar de otros métodos menos invasivos y en el que solicitaba que en el momento de la toma de los datos biométricos, se dé debido cumplimiento a todos y cada uno de los requisitos establecidos por la normativa vigente sobre protección de datos personales, especialmente que se facilite por escrito la información prevista en el art. 13 y arts. 3 y 11 del Reglamento General de Protección de Datos.

- Con fecha de 12/5/22 el Ayuntamiento contesta al escrito dándole cita para la toma de datos biométricos para el 19/05/2022, sin contestar a la parte referida a la revisión de la legalidad de los sistemas biométricos implantados que la reclamante incluyó en su escrito.

- Manifiesta la parte reclamante que el día de la fecha de toma de datos biométricos, 19/05/22, le comunicaron verbalmente que se cancelaba la toma de datos hasta nueva orden.

Junto a la reclamación, aporta los escritos referenciados en la reclamación.

SEGUNDO: Con fecha de 27-12-2022 se dicta resolución de inadmisión a trámite de la reclamación presentada por falta de acreditación de indicios suficientes de haberse implantado el sistema biométrico de reconocimiento facial del Ayuntamiento.

TERCERO: Con fecha de 23-01-2023 se interpone recurso de reposición contra la inadmisión a trámite, en el que se aporta nueva documentación. Recurso que se resuelve mediante Resolución de 17-04-2023, en la que se resuelve estimar el recurso interpuesto y admitir a trámite la reclamación presentada, a la vista de que: "*junto al recurso de reposición se ha aportado nueva documentación relevante a los efectos de lo planteado, que debe ser analizada por la Subdirección General de Inspección de Datos."*

CUARTO: En cumplimento de dicha resolución, la Subdirección General de Inspección de Datos procedió a iniciar actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, dentro del cual se han realizado las siguientes actuaciones:

Realizado requerimiento de información al Ayuntamiento reclamado el día 27 de abril, 19 de mayo y 14 de julio de 2023, se recibe respuesta del mismo con fecha de 20 de julio de 2023 donde, manifiesta, resumidamente, lo siguiente:

- Reconoce haber implantado el sistema de fichaje por huella dactilar desde el año 2015.

- Respondiendo a la cuestión referida a los tratamientos realizados y a la fecha de inicio de los mismos, el Ayuntamiento indica lo siguiente:

  > *"Con fecha 19/10/2021 se emitió circular de la Concejala de Economía, Hacienda y Recursos Humanos, sobre la implantación de un sistema de control horario denominado TARA (Tiempo aplicado a Recursos y Acciones). Se insta a los empleados a realizar los fichajes a través de los correspondientes terminales (excepcionalmente, para el personal que se encuentra temporalmente en trabajo no presencial, hasta la vuelta a la presencialidad, se habilitó el control a través del ordenador – web).*
  >
  > *Desde el 02/11/2021 se insta a realizar los fichajes con el nuevo sistema, así como a partir del 01/01/2022 a realizar las gestiones de licencias, permisos y vacaciones. A este particular, el Reglamento del Control Horario no fue aprobado definitivamente hasta el acuerdo plenario del 31/03/2022 y publicación en el BOP nº 41 de 06/04/2022.*
  > *La implantación del sistema de control horario se efectuó, básicamente, a través de terminales por reconocimiento facial, toda vez la situación de crisis sociosanitaria del COVID, además, por ello se implantó la gestión laboral de teletrabajo.*
  > *El control horario es un procedimiento de implantación progresiva, que además de la instalación de terminales de fichajes, deben gestionarse los diferentes servicios para el detalle de jornadas especiales, la planificación de instalación de nuevos terminales, la formación de los/as empleados/as, la resolución de los problemas lógicos de implantación, etc."*

- Preguntado por si solicitó informe al Delegado de Protección de Datos (en adelante, DPD) previamente a iniciar las nuevas operaciones de tratamiento previstas para el fichaje de la jornada en las mencionadas normas municipales, el Ayuntamiento manifiesta que: "*No se solicitó informe del Delegado de Protección de Datos previamente al inicio de los citados tratamientos, existiendo un informe de fecha de 24 de noviembre de 2020 referente a idoneidad en relación a la posibilidad de implantación del fichaje laboral mediante reconocimiento facial en relación a las medidas higiénicas que se deben aplicar por la situación sanitaria por pandemia COVID19 cuando se trata de verificación/autenticación biométrica (uno-a-uno*).

  Se adjunta dicho informe PRODAT emitido por el Delegado de Protección de Datos de 24/11/2020 sobre la idoneidad de la implantación del fichaje laboral mediante el reconocimiento facial, y copia del Informe jurídico AEPD 36/2020 sobre el uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online partiendo de que el estado de alarma declarado por Real Decreto 463/2020, de 14 de marzo.

- Manifiesta que no ha realizado una Evaluación de Impacto relativa a la protección de datos del tratamiento.

- Por último, indica que no todos los/as empleados/as disponen de dispositivo móvil corporativo para efectuar el fichaje mediante geolocalización, habiéndoselo instalado en sus dispositivos móviles personales aquellos empleados que se mostraban disponibles, voluntariamente. Recientemente, se ha comenzado a dotar de teléfonos móviles corporativos y tarjeta SIM a los empleados que fichan por esta modalidad.

Junto con su escrito de alegaciones, el Ayuntamiento acompaña la normativa municipal mencionada, los certificados ENS_MHP, e ISO_27001_MHP, y los Informes PRODAT y de la AEPD arriba referenciados.

Se observa que los certificados aportados por el Ayuntamiento constan expedidos por la entidad MHP SERVICIOS DE CONTROL, S.L (en adelante MHP), y que en el proyecto de Reglamento Municipal se dice haber suscrito un contrato de encargo del tratamiento con la misma. Por este motivo, se formula un requerimiento a MHP con fecha de 26 de junio de 2023, requiriendo a la misma aporte contrato de encargado de tratamiento suscrito con el Ayuntamiento, y el Registro de Actividades de Tratamiento para los tratamientos de fichaje por reconocimiento facial y geolocalización a través de móvil, y solicitando informe acerca de si para el fichaje a través de geolocalización se utilizaba un teléfono móvil personal o corporativo.

Con fecha de 6 de julio de 2023, se presentan alegaciones por parte de MHP, en las que se reconoce haber sido contratado por el Ayuntamiento como encargado del tratamiento para la implantación del sistema TARA de gestión de horario. En su escrito, MHP:

- Aporta dos contratos de encargado de tratamiento suscritos con el Ayuntamiento, de fechas 2-3-20 y 2-8-21, y los correos intercambios para la contratación. (DOCS 2 a 4).

- Respecto al Registro de Actividades de Tratamiento, se aportan los dos que fueron elaborados con ocasión de cada contrato para el reconocimiento facial y el sistema de geolocalización, tal y como se requiere. (DOCS 5 a 7). Respecto a si el sistema de geolocalización por móvil se instalaba en un móvil personal o corporativo: indica que es el responsable del tratamiento el único que puede informar al respecto. No obstante se hace constar por MHP, que ésta recomendó la utilización de terminales móviles corporativos y no personales de los trabajadores, tal y como aparece en el Protocolo de Implantación del Sistema Integral de Control Horario, (DOC 8), que se adjuntó al contrato suscrito con el Ayuntamiento.

  Todo ello, en base a la interpretación que MHP realiza de la sentencia dictada por la Audiencia Nacional del 6 de febrero de 2019 "Caso Telepizza", ratificada por el Tribunal Supremo, en la que se confirmó que la empresa no puede obligar a los

repartidores a conectar sus propios móviles a aplicaciones informáticas de la empresa para facilitar su geolocalización durante el reparto.

Se observa que el “Protocolo de Implantación del Sistema Integral de Control Horario, edición octubre 2022”, aprobado por la DPD de MHP, y aportado como DOCUMENTO 8, que MHP dice haber adjuntado al contrato suscrito con el Ayuntamiento, contiene en su punto 13 un apartado de modelos sugeridos para utilizar por el responsable del tratamiento, entre los que se encuentran, las cláusulas informativas de todas las alternativas de fichaje y el consentimiento informado, y un modelo posible EIPD sobre el tratamiento de datos personales relacionados con los sistemas de fichaje implantados.

Con fecha de 22-11-23 se dicta Diligencia de la Inspectora en la que se hace constar que, tras una búsqueda, se une al expediente la información que se encuentra sobre el Registro de Actividades de Tratamiento (RAT) en el apartado de Transparencia de la página web del ayuntamiento, https://www.telde.es/wpcontent/uploads/2022/07/RAT_Entidad_Publica_v3__MI-AYUNTAMIENTO-DE-TELDE.pdf, Ref. v. Gen. 08-01-2020, Autor PRODAT.

Por último, con fecha de 18 de diciembre de 2023 la inspectora emite Informe de Actuaciones Previas, emitiendo sus conclusiones al respecto de lo actuado.

De toda la documentación aportada durante la fase de actuaciones previas, se desprende la siguiente **cronología de los hechos** que se derivan de las actuaciones practicadas:

-2015: Implantación del sistema de fichaje por huella dactilar.

-2/3/2020: El Ayuntamiento decide implantar un nuevo sistema de fichaje de sus empleados municipales, y aprueba un contrato inicial para encargar el tratamiento de datos personales a la entidad MHP.

-2/8/2021: El Ayuntamiento suscribe un segundo y último contrato de encargado de tratamiento con MHP.

-19/10/2021: Se dicta la Circular de la Concejalía de Economía, Hacienda y RRHH, sobre el control de asistencia de los/as empleados/as municipales, y se comunica a los empleados que van a comenzar los fichajes de reconocimiento facial en fase de prueba, y de forma definitiva a partir de la aprobación de un Reglamento.

-2/11/2021: Según reconoce el Ayuntamiento en sus alegaciones, comienzan los fichajes en fase de prueba, tal y como se indicaba en la Circular.

-19/11/2021: Acta de la Mesa General de Negociación con los representantes sindicales de los trabajadores, de aprobación del Reglamento de la Jornada Laboral y de la Gestión de Permisos del Personal Municipal del Ayuntamiento de Telde.

-16/12/2021: Certificado de acuerdo de JGL (Junta de Gobierno Local) de aprobación del Proyecto de Reglamento Regulador de la jornada laboral y de la gestión de permisos del personal municipal del Ayuntamiento de TELDE.

-27/12/2021: Certificado de acuerdo Plenario del Ayuntamiento de Aprobación inicial del Reglamento horario.

-3/1/2022: Publicación en el BOP N.º 1 (Boletín Oficial de la Provincia de las Palmas). Sometimiento a información pública del Reglamento horario.

-31/3/2022: Certificado de acuerdo Plenario sobre Aprobación definitiva del Reglamento horario.

- 6/4/2022: Publicación en el BOP N.º 41. Que supone la entrada en vigor del Reglamento horario según la D.F 3ª del mismo.

CUARTO: Con fecha 15 de abril de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del Artículo 38 del RGPD, Artículo 9 del RGPD y Artículo 35 del RGPD, tipificada en el Artículo 83.4.a) del RGPD y Artículo 83.5.a) del RGPD.

En el citado Acuerdo de inicio se acordaba:

*"ORDENAR como medida provisional al **AYUNTAMIENTO DE TELDE**, con NIF **P3502600D**, de acuerdo con lo dispuesto en el artículo 69 de la LOPDGDD y artículo 56 de la LPACAP, la suspensión temporal de todo tratamiento de datos personales correspondiente a los sistemas de fichaje biométrico-y en especial de los referidos al sistema de reconocimiento facial- y fichaje a través de APP en el móvil con geolocalización de sus empleados como método de control de cumplimiento de la jornada laboral de sus empleados.*

La medida provisional deberá llevarse a cabo en el plazo de diez días hábiles, contados desde la notificación de este acuerdo de apertura del procedimiento, y permanecerá hasta su resolución final, en que deberá ser confirmada, modificada o levantada, sin perjuicio de lo dispuesto en el art. 56.5 de la LPACAP, pudiendo acordarse en la resolución final la limitación definitiva o prohibición de dichas operaciones de tratamiento de acuerdo con lo previsto en los artículos 58 del RGPD y 69 de la LOPDGDD. A tal fin, deberá justificar ante esta Agencia Española de Protección de Datos la atención del presente requerimiento."

El Ayuntamiento de Telde no ha acreditado hasta el momento haber ejecutado esta medida de suspensión provisional.

QUINTO: Notificado el citado acuerdo de inicio a la entidad reclamada con fecha de 17 de abril de 2024 conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), tal y como consta en acuse de recibo en el expediente, y transcurrido el plazo otorgado para la formulación de alegaciones, se ha constatado que no se ha recibido alegación alguna por la parte reclamada.

El artículo 64.2.f) de la LPACAP -disposición de la que se informó a la parte reclamada en el acuerdo de apertura del procedimiento- establece que si no se efectúan alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, cuando éste contenga un pronunciamiento preciso acerca de la responsabilidad imputada, podrá ser considerado propuesta de resolución. En el presente caso, el acuerdo de inicio del expediente sancionador determinaba los hechos en los que se concretaba la imputación, la infracción del RGPD atribuida a la reclamada y la sanción que podría imponerse. Por ello, tomando en consideración que la parte reclamada no ha formulado alegaciones al acuerdo de inicio del expediente y en atención a lo establecido en el artículo 64.2.f) de la LPACAP, el citado acuerdo de inicio es considerado en el presente caso propuesta de resolución.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes

HECHOS PROBADOS

PRIMERO: De acuerdo con las propias manifestaciones realizadas por la entidad reclamada en su escrito de 20 de julio de 2023 por el que contesta al traslado realizado por esta Agencia en el marco del presente procedimiento, el Ayuntamiento dispone desde el año 2015 de un sistema de fichaje por huella dactilar de sus empleados como medio de control de cumplimiento de la jornada laboral de sus empleados municipales. Se indica al respecto lo siguiente: "*Desde 2015 se venía realizando tratamiento de datos biométricos a través de huella dactilar, siendo sustituido dicho dato biométrico por el de reconocimiento facial, a raíz de las circunstancias sanitarias derivadas de la pandemia de COVID-19, siendo aprobado en Mesa General de Negociación por los diferentes representantes de los trabajadores".*

SEGUNDO: El Ayuntamiento confirma que a partir del 2 de noviembre de 2021 comenzó a implantar un nuevo sistema de control de horario laboral de sus empleados denominado TARA (Tiempo aplicado a recursos y acciones), iniciando un nuevo tratamiento de datos personales con la finalidad de registrar y controlar el cumplimiento de la jornada laboral, contratado con la entidad MHP SERVICIOS DE CONTROL, S.L (en adelante MHP), como encargada del tratamiento.

Así pues, de acuerdo con lo manifestado y acreditado por el propio Ayuntamiento en su escrito de 20 de julio de 2023, por el que contesta al traslado realizado por esta Agencia, en su punto segundo, referido a la "Confirmación de la aplicación de los citados tratamientos, indicando fecha de inicio", el Ayuntamiento reconoce los siguientes hechos: **"***Con fecha 19/10/2021 se emitió circular de la Concejala de Economía, Hacienda y Recursos Humanos, sobre la implantación de un sistema de control horario denominado TARA (Tiempo aplicado a Recursos y Acciones). Se insta a los empleados a realizar los fichajes a través de los correspondientes terminales (excepcionalmente, para el personal que se encuentra temporalmente en trabajo no presencial, hasta la vuelta a la presencialidad, se habilitó el control a través del ordenador – web). Desde el 02/11/2021 se insta a realizar los fichajes con el nuevo sistema, así como a partir del 01/01/2022 a realizar las gestiones de licencias, permisos y vacaciones. A este particular, el Reglamento del Control Horario no fue*

aprobado definitivamente hasta el acuerdo plenario del 31/03/2022 y publicación en el BOP nº 41 de 06/04/2022.La implantación del sistema de control horario se efectuó, básicamente, a través de terminales por reconocimiento facial, toda vez la situación de crisis sociosanitaria del COVID, además, por ello se implantó la gestión laboral de teletrabajo. El control horario es un procedimiento de implantación progresiva, que además de la instalación de terminales de fichajes, deben gestionarse los diferentes servicios para el detalle de jornadas especiales, la planificación de instalación de nuevos terminales, la formación de los/as empleados/as, la resolución de los problemas lógicos de implantación, etc."

TERCERO: De los documentos aportados por el propio Ayuntamiento en su escrito de 20 de julio de 2023 y la encargada del tratamiento MHP en su escrito de 6 de julio de 2023 se desprende que el proceso de implantación de este nuevo Sistema TARA se realizó de forma progresiva, de acuerdo con la siguiente cronología:

-2/3/2020: El Ayuntamiento aprueba un contrato inicial para encargar el tratamiento de datos personales a la entidad MHP en relación con la prestación del Servicio Integral de la Gestión de Horarios, cuyo objeto y finalidad el fijado en su cláusula primera, que dispone lo siguiente: "*A medio del presente acuerdo, se pretende definir y establecer el régimen jurídico aplicable al tratamiento de los datos personales que se encuentren bajo la responsabilidad del cliente, y que a instancias de éste, requieran ser tratados por MHP Servicios de Control S.L, para llevar a cabo la prestación del Servicio Integral de Gestión de Horarios contratad*o"**.** Lo que se realiza en la cláusula segunda del Contrato de encargo, que determina que**:** "*Para llevar a buen término la prestación del Servicio Integral de la Gestión de Horarios, el Responsable del Tratamiento pondrá a disposición del Encargado del Tratamiento, sólo los siguientes datos personales de cada uno de sus usuarios:*
a) Nombre y apellidos.
b) Documento nacional de identidad.
c) Minucia de huella y su código numérico asociado, asignado por el cliente o en su defecto por MHP.
d) Datos relativos al puesto de trabajo: Departamento, categoría, turno, etc.
e) Email del usuario.
f) En su caso, un código pin generado por MHP de forma aleatoria asociado al trabajador, un número de teléfono asignado por el Responsable para llevar a cabo el fichaje telefónico y si procediera, su geolocalización, y en caso de fichar a través de tarjeta, un código numérico que identifique al usuario.
La recogida del dato biométrico se realizará en las instalaciones del Responsable del Tratamiento, y se llevará a cabo a través de los dispositivos hardware propiedad del Encargado del Tratamiento, quien mediante acceso remoto, los incorporará a sus sistemas de información ubicados en las instalaciones centrales del Encargado del Tratamiento, donde serán tratados para la prestación efectiva del servicio".

-2/8/2021: Firma de un segundo contrato de encargo de tratamiento con MHP. De acuerdo con las manifestaciones realizadas por MHP en su escrito de 6 de julio de 2023, punto primero: *"dado que con ocasión de la crisis sanitaria del Covid-19, el mercado nacional demandaba implantar otras alternativas de fichaje, MHP desarrolló entre sus opciones comerciales el dispositivo de fichaje (terminal) a través del reconocimiento facial. Mostrando el Ayuntamiento de Telde interés por*

*contar con esta nueva alternativa, se procede a la actualización del contrato de tratamiento de datos, el cual se adjunta a los efectos probatorios oportunos como documento número CUATRO**,** y en el que se especifica expresamente, el tratamiento del dato biométrico huella/facial*"**.**

De acuerdo con la cláusula segunda del citado contrato, las partes acuerdan ampliar los datos personales que se podrán a disposición del encargado del tratamiento, en función de la posible modalidad de fichaje de la jornada laboral que fuera elegida por el Ayuntamiento, en los siguientes términos:

"Para llevar a buen término la prestación del Servicio Integral de la Gestión de Horarios, el Responsable del Tratamiento pondrá a disposición del Encargado del Tratamiento, única y exclusivamente los siguientes datos personales de cada uno de sus usuarios en función de la modalidad de fichaje que haya sido elegida:

"I.- Fichaje Biométrico (huella/reconocimiento facial) a través de Dispositivo TRD y/o hámster: nombre, apellidos, DNI, datos relativos al puesto de trabajo (departamento, categoría, turno, etc), correo electrónico del usuario, minucia huella/patrón facial con su código numérico asociado, y en su caso, código pin.

La recogida del dato biométrico se realizará en las instalaciones del Responsable del Tratamiento, y se llevará a cabo a través de los dispositivos hardware propiedad del Encargado del Tratamiento, quien mediante acceso remoto, los incorporará a sus sistemas de información ubicados en sus instalaciones centrales, sitas en Las Palmas de Gran Canaria, donde serán tratados para la prestación efectiva del servicio.

II. Fichaje a través de la tarjeta magnética y/o proximidad: *nombre, apellidos, DNI, datos relativos al puesto de trabajo (departamento, categoría, turno, etc), correo electrónico, y código numérico asociado al usuario.*

III. Fichaje telefónico: *nombre, apellidos, DNI, datos relativos al puesto de trabajo (departamento, categoría, turno, etc), correo electrónico, y número de teléfono asignado al usuario que previamente le hubiere asignado el Responsable del tratamiento.*

IV.- Fichaje App Móvil Geogestión con geolocalización: *nombre, apellidos, DNI, datos relativos al puesto de trabajo (departamento, categoría, turno, etc), correo electrónico, los datos del dispositivo móvil (código alfanumérico id único que se genera por la combinación del dispositivo y la aplicación Geogestión Horaria),y su geolocalización detallando las coordenadas de la ubicación del usuario, que solo se activará y recabará, en el momento en el que se realice el fichaje.*

V. IV.- Fichaje App Móvil Geogestión sin geolocalización: *nombre, apellidos, DNI, datos relativos al puesto de trabajo (departamento, categoría, turno, etc), correo electrónico, los datos del dispositivo móvil (código alfanumérico id único que se genera por la combinación del dispositivo y la aplicación Geogestión Horaria),*

VI.- Fichaje mediante enlace web: nombre, apellidos, DNI, datos relativos al puesto de trabajo (departamento, categoría, turno, etc), correo electrónico, código numérico asociado a un identificador único universal del equipo, asignado al usuario y en su caso, la Ip pública asociada y asignada por el Responsable del Tratamiento".

-19/10/2021: Se dicta la Circular de la Concejalía de Economía, Hacienda y RRHH, sobre el control de asistencia de los/as empleados/as municipales, en la que se indica lo siguiente:

"(…) Se va a implantar un nuevo sistema de control de horario denominado ***TARA*** *(Tiempo Aplicado a Recursos y Acciones). Los fichajes diarios en el sistema Tara se tendrán que realizar en los terminales instalados en las respectivas dependencias municipales, solo permitiendo el fichaje en el terminal ubicado en la dependencia donde se prestan los servicios. Excepcionalmente, para el personal que se encuentra temporalmente en trabajo no presencial, hasta la vuelta a la presencialidad, se ha habilitado el control a través de ordenador.*

Desde el próximo día 2 de Noviembre de 2021 se procederá a realizar los fichajes con este nuevo sistema, en fase de prueba.
A partir del 1 de Enero de 2022, una vez aprobado el Reglamento Regulador del control Horario, se realizarán además todas las gestiones de solicitud de compensaciones, licencias, permisos y vacaciones con este sistema. Se les irá informando de la implantación a medida que vayamos avanzando en las fases de la misma".

-2/11/2021: Según reconoce el Ayuntamiento en su escrito de 20 de julio de 2023, comienzan los fichajes de acuerdo con el nuevo sistema de reconocimiento facial utilizando los terminales situados en cada dependencia del mismo para los fichajes de tipo presencial, y habilitándose el sistema de conexión web para los supuestos de teletrabajo autorizados durante la pandemia del Covid-19.

- 6/4/2022: Publicación y entrada en vigor del Reglamento de la Jornada Laboral y de la Gestión de Permisos del Personal Municipal del Ayuntamiento de Telde, según la D.F 3ª del mismo (BOP N.º 41). Tras haber sido acordado por la Mesa General de Negociación con los representantes sindicales de los trabajadores con fecha de 19-11-21, y aprobado de forma definitiva el 31-3-22 por el Pleno del Ayuntamiento.

De acuerdo con su artículo 1: "*El presente Reglamento tiene por objeto regular los medios, actuación, criterios y procedimientos a seguir para el control del cumplimiento de la jornada de trabajo y del horario flexible, implementados mediante la aplicación informática denominada Tiempo Aplicado a Recursos y Acciones (en adelante, TARA), como sistema para la gestión de los procedimientos en materia de personal, relacionados con vacaciones, permisos, licencias, jornada y horario de trabajo que afectan al personal al servicio de la Administración del Ayuntamiento de Telde".*

Y en su artículo 11 el Reglamento señala lo siguiente sobre las modalidades de fichaje de la de la jornada, que denomina como "fichaje electrónico":

"*Artículo 11.- Sistema de control horario.*
1. Sin perjuicio de la utilización de cualquier otro método, procedimiento o sistema de control de permanencia que se pudiera establecer, a los efectos del presente reglamento se podrán utilizar para el fichaje electrónico los siguientes medios y sistemas:
a) El Reconocimiento Facial.
b) Mediante Internet, a través de la web habilitada al efecto
c) El reconocimiento mediante la geolocalización.
2. Todas las unidades administrativas, deberán contener un dispositivo de control horario, mediante reconocimiento facial, atendiéndose, en cada caso, a las peculiaridades de las dependencias en las que se encuentre ubicadas (el subrayado es de la AEPD)
3. En aquellos casos y centros de trabajo que no dispongan dispositivos de control horario, mediante reconocimiento facial, por sus peculiaridades, por ser gravosos o de extrema dificultad la implantación, el personal deberá fichar mediante dispositivos de geolocalización o, en su defecto, conforme a las indicaciones que a tal efecto sean emitidas por el servicio de Recursos Humanos."

CUARTO: Por lo que respecta al fichaje mediante APP móvil Geogestión con geolocalización, el Ayuntamiento confirma su aplicación efectiva, reconociendo en el punto quinto de su escrito de respuesta al traslado de 20 de julio de 2023 lo siguiente: *" 5º).- Fichaje a través de móvil con geolocalización. Realización mediante móvil corporativo o personal del empleado/a municipal. Indicar que no todos los/as empleados/as disponen de dispositivo móvil corporativo. Por ello, aquellos que han mostrado su disponibilidad, han instalado en sus dispositivos móviles personales la aplicación correspondiente para efectuar el fichaje mediante geolocalización. Al respecto, a ningún trabajador/a se le ha obligado a la instalación de la aplicación, y en caso de negativa, circunstancia mínima, en la medida de lo posible se ha gestionado realizando el fichaje en terminal*."*Finalmente, no ha existido constancia de disconformidad de todos los/as trabajadores/as a los que se le instaló la aplicación de fichaje geolocalización. Si nos consta solicitud de realizar el fichaje a través de móvil en sustitución de terminal, siendo gestionado por Recursos Humanos conforme al Reglamento del Control Horario y las dependencias/servicios de los/as respectivos/as solicitantes (mayormente de forma verbal).*

QUINTO: Consta en el procedimiento la siguiente documentación que acredita que el Ayuntamiento del Telde es la entidad responsable del tratamiento de datos personales realizado para el control de presencia y registro de jornada laboral de sus empleados, y la entidad MHP es la encargada del tratamiento::

- De la suscripción de los dos contratos de encargo del tratamiento de 2020 y 2021 entre Ayuntamiento y MHP. En ambos documentos contractuales la cláusula cuarta define las obligaciones del "responsable del tratamiento" y "encargado del tratamiento". Y se contiene una cláusula primera que señalan lo siguiente: "*PRIMERO.- Objeto y finalidad del presente contrato de Encargo del Tratamiento", en cuyo párrafo segundo se hace constar que: "Sea como fuere, el tratamiento de los datos por parte del Encargado del Tratamiento, se limitará a las actuaciones necesarias para desarrollar correctamente el servicio, siguiendo las instrucciones documentadas que, en cada caso, le dirija el Responsable del*

Tratamiento, tal y como exige el vigente Reglamento Europeo (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, en adelante RGPD y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)".

- Reglamento de jornada laboral de 31/03/21, que señala en su artículo 3, las siguientes normas aplicables en materia de tratamiento de datos personales: "*Artículo 3.-Tratamiento de los datos personales 1. Cualquier sistema que se utilice para el control horario o control y gestión de los permisos y licencias, deberá adecuarse a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y al Reglamento (UE) 2016/679 del Parlamento Europeo y Consejo de 27 de abril de 2016. 2. El Ayuntamiento de deberá informar de forma expresa, clara e inequívoca a los trabajadores/as, acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión. 3. Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación a los fines para los que son tratados (minimización de datos), exactos y si fuera necesario actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan".*

SEXTO: El Ayuntamiento ha estado tratando datos personales biométricos (mediante sistemas de huella dactilar y reconocimiento facial) y datos personales de localización (a través de APP con geolocalización en el dispositivo móvil personal de los empleados), sin haber realizado y superado previamente una EIPD, ni en el momento previo a su implantación ni posteriormente, tal y como reconoce en el punto 4 de su escrito de contestación al traslado de 20 de julio de 2023, que indica lo siguiente: *"4º).- Documento de evaluación de Impacto de Protección de Datos de los citados tratamientos. No se posee una evaluación de Impacto de Protección de Datos de los citados tratamientos".*

SÉPTIMO: El Ayuntamiento no ha aportado justificación documental que permita acreditar la concurrencia de ninguna de las excepciones previstas del artículo 9.2 del RGPD que permita tratar datos biométricos como medio de control de la obligación legal de vigilar y controlar la jornada laboral de los empleados municipales.

OCTAVO: Consta que el DPD del Ayuntamiento -cuya designación era obligatoria-no participó ni fue previamente consultado por el Ayuntamiento en ninguna de las fases de implantación de este tratamiento, ni previamente, ni durante, ni posteriormente al inicio de las ninguna de las 3 operaciones de tratamiento llevadas a cabo para controlar el horario de sus empleados municipales a partir del 2-11-21.

El Ayuntamiento reconoce claramente que: "*No se solicitó informe del Delegado de Protección de Datos previamente al inicio de los citados tratamientos, existiendo un informe de fecha de 24 de noviembre de 2020 referente a idoneidad en relación a la posibilidad de implantación del fichaje laboral mediante reconocimiento facial en relación a las medidas higiénicas que se deben aplicar por la situación sanitaria por pandemia COVID19 cuando se trata de verificación/autenticación biométrica (uno-a-uno)"*

El citado Informe PRODAT de 24/11/2020 aportado por el Ayuntamiento, no contiene pie de firma ni se identifica a la persona u órgano emisor. Además, y ciñe su objeto de análisis es el siguiente: "*Habiéndose realizado la consulta por parte del M.I. AYUNTAMIENTO DE TELDE en relación a la idoneidad de la implantación del fichaje laboral mediante el reconocimiento facial, se debe analizar si la implantación del sistema de reconocimiento facial es conforme a la normativa estatal vigente de protección de datos de carácter personal".*

FUNDAMENTOS DE DERECHO

I. Competencia y procedimiento

De acuerdo con los poderes que el artículo 58.2 del RGPD y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, 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. Cuestiones previas

2.1. Descripción del sistema de control de jornada/horario del personal implantado por el Ayuntamiento.

De acuerdo con la documentación obrante en el procedimiento, y lo manifestado por el propio Ayuntamiento y encargado del tratamiento, el Ayuntamiento implantó, de forma progresiva, un nuevo sistema de control de horario denominado TARA que fijó los sistemas de fichaje que serían aplicables para controlar el horario de la jornada laboral de los empleados municipales, a través de diferentes normas municipales:

- Con fecha de 10-1-21 se dicta la Circular de la Concejalía de Economía, Hacienda y RRHH, sobre el control de asistencia de los/as empleados/as municipales, en la que se comunica a los empleados que:

  > *"(…) Se va a implantar un nuevo sistema de control de horario denominado* ***TARA*** *(Tiempo Aplicado a Recursos y Acciones). Los fichajes diarios en el sistema Tara se tendrán que realizar en los terminales instalados en las respectivas dependencias municipales, solo permitiendo el fichaje en el terminal ubicado en la dependencia donde se prestan los servicios. Excepcionalmente, para el personal que se encuentra temporalmente en trabajo no presencial, hasta la vuelta a la presencialidad, se ha habilitado el control a través de ordenador.*

Desde el próximo día 2 de Noviembre de 2021 se procederá a realizar los fichajes con este nuevo sistema, en fase de prueba.
A partir del 1 de Enero de 2022, una vez aprobado el Reglamento Regulador del control Horario, se realizarán además todas las gestiones de solicitud de compensaciones, licencias, permisos y vacaciones con este sistema. Se les irá informando de la implantación a medida que vayamos avanzando en las fases de la misma".

- Las alegaciones del Ayuntamiento amplían dicha información, de las que se deducen los siguientes hechos relevantes para el presente procedimiento:

  - Desde el año 2015 el sistema utilizado para el fichaje era por medio de huella dactilar, sin realizar más manifestaciones al respecto.
  - El denominado "nuevo sistema de fichaje realizado a través de los correspondientes terminales" al que se refiere la Circular es el de reconocimiento facial, que se fija como sistema común de fichaje o regla general.
  - Excepcionalmente, para el personal que se encuentra temporalmente en trabajo no presencial, hasta la vuelta a la presencialidad, se habilitó el control a través del ordenador – web"
  - Los sistemas 2 implantados a través de la Circular comenzaron el 2/11/21 en "fase de pruebas".
  - Pese a que se indica que a partir del 1/1/22 se realizarán conforme a la aplicación TARA las gestiones de licencias, permisos y vacaciones, el Ayuntamiento indica que "el *Reglamento del Control Horario no fue aprobado definitivamente hasta el acuerdo plenario del 31/03/2022 y publicación en el BOP nº 41 de 06/04/2022*."

- Según la Disposición Final 3ª de dicho Reglamento de Control de Horario, éste entró en vigor el día de su publicación en el BOP (6-4-22), y amplió a 3 los sistemas de "fichaje electrónico" de los empleados municipales. En lo que respecta a los sistemas de fichaje implantados, destaca en especial el artículo 11, que indica lo siguiente:

  "*Artículo 11.- Sistema de control horario.*
  1. Sin perjuicio de la utilización de cualquier otro método, procedimiento o sistema de control de permanencia que se pudiera establecer, a los efectos del presente reglamento se podrán utilizar para el fichaje electrónico los siguientes medios y sistemas:
  a) El Reconocimiento Facial.
  b) Mediante Internet, a través de la web habilitada al efecto
  c) El reconocimiento mediante la geolocalización.
  2. Todas las unidades administrativas, deberán contener un dispositivo de control horario, mediante reconocimiento facial, atendiéndose, en cada caso, a las peculiaridades de las dependencias en las que se encuentre ubicadas (el subrayado es de la AEPD)
  3. En aquellos casos y centros de trabajo que no dispongan dispositivos de control horario, mediante reconocimiento facial, por sus peculiaridades, por ser gravosos o de extrema dificultad la implantación, el personal deberá fichar mediante dispositivos de geolocalización o, en su defecto, conforme a las

indicaciones que a tal efecto sean emitidas por el servicio de Recursos Humanos."

Ambas normas fueron precedidas por dos contratos de encargo del tratamiento con la entidad MHP, que han sido aportados al procedimiento, con la finalidad de implantar el nuevo sistema de gestión integral de control de horario denominado TARA.

- Con fecha de 2/3/20, el Ayuntamiento aprueba un contrato inicial para encargar el tratamiento de datos personales a la entidad MHP en relación con la prestación del Servicio Integral de la Gestión de Horarios, cuyo objeto y finalidad el fijado en su cláusula primera, que dispone lo siguiente: "*A medio del presente acuerdo, se pretende definir y establecer el régimen jurídico aplicable al tratamiento de los datos personales que se encuentren bajo la responsabilidad del cliente, y que a instancias de éste, requieran ser tratados por MHP Servicios de Control S.L, para llevar a cabo la prestación del Servicio Integral de Gestión de Horarios contratado*"**.**

  A estos efectos, la cláusula segunda del Contrato de encargo señalaba los datos personales que era preciso tratar para poder implantar sistemas de fichaje biométrico (limitado aun a la huella dactilar), así como sistemas de fichaje por geolocalización, pero no se concretaban con claridad en el contrato las posibles modalidades de fichaje de la jornada laboral que iban a ser objeto de tratamiento.

  En concreto, dicha cláusula determina que**:** "*Para llevar a buen término la prestación del Servicio Integral de la Gestión de Horarios, el Responsable del Tratamiento pondrá a disposición del Encargado del Tratamiento, sólo los siguientes datos personales de cada uno de sus usuarios:*

- *a) Nombre y apellidos.*
- *b) Documento nacional de identidad.*
- *c) Minucia de huella y su código numérico asociado, asignado por el cliente o en su defecto por MHP.*
- *d) Datos relativos al puesto de trabajo: Departamento, categoría, turno, etc.*
- *e) Email del usuario.*
- *f) En su caso, un código pin generado por MHP de forma aleatoria asociado al trabajador, un número de teléfono asignado por el Responsable para llevar a cabo el fichaje telefónico y si procediera, su geolocalización, y en caso de fichar a través de tarjeta, un código numérico que identifique al usuario.*
- *La recogida del dato biométrico se realizará en las instalaciones del Responsable del Tratamiento, y se llevará a cabo a través de los dispositivos hardware propiedad del Encargado del Tratamiento, quien mediante acceso remoto, los incorporará a sus sistemas de información ubicados en las instalaciones centrales del Encargado del Tratamiento, donde serán tratados para la prestación efectiva del servicio*".

- El segundo contrato de encargo con MHP fue suscrito el 2-8-21. De acuerdo con las manifestaciones realizadas por MHP en su escrito de 6 de julio de 2023, punto primero, la suscripción de un nuevo contrato se debió a: *" que con ocasión de la crisis sanitaria del Covid-19, el mercado nacional demandaba implantar otras alternativas de fichaje, MHP desarrolló entre sus opciones comerciales el*

*dispositivo de fichaje (terminal) a través del reconocimiento facial. Mostrando el Ayuntamiento de Telde interés por contar con esta nueva alternativa, se procede a la actualización del contrato de tratamiento de datos, el cual se adjunta a los efectos probatorios oportunos como documento número CUATRO**,** y en el que se especifica expresamente, el tratamiento del dato biométrico huella/facial*"**.**

Así pues, con el objeto de ampliar las modalidades posibles de fichaje de la jornada al reconocimiento facial, la cláusula segunda de este contrato determinó los datos personales que debían ser objeto de tratamiento en cada una de las modalidades de fichaje de las que disponía el sistema desarrollado por el encargado MHP, y desarrolló con detalle 6 posibles modalidades de fichaje de la jornada laboral que se incluían dentro del contrato.

En esta línea, esta cláusula segunda dispuso lo siguiente: *"Para llevar a buen término la prestación del Servicio Integral de la Gestión de Horarios, el Responsable del Tratamiento pondrá a disposición del Encargado del Tratamiento, única y exclusivamente los siguientes datos personales de cada uno de sus usuarios en función de la modalidad de fichaje que haya sido elegida:*

"I.- Fichaje Biométrico (huella/reconocimiento facial) a través de Dispositivo TRD y/o hámster: nombre, apellidos, DNI, datos relativos al puesto de trabajo (departamento, categoría, turno, etc), correo electrónico del usuario, minucia huella/patrón facial con su código numérico asociado, y en su caso, código pin.

La recogida del dato biométrico se realizará en las instalaciones del Responsable del Tratamiento, y se llevará a cabo a través de los dispositivos hardware propiedad del Encargado del Tratamiento, quien mediante acceso remoto, los incorporará a sus sistemas de información ubicados en sus instalaciones centrales, sitas en Las Palmas de Gran Canaria, donde serán tratados para la prestación efectiva del servicio.

II. Fichaje a través de la tarjeta magnética y/o proximidad: *nombre, apellidos, DNI, datos relativos al puesto de trabajo (departamento, categoría, turno, etc), correo electrónico, y código numérico asociado al usuario.*

III. Fichaje telefónico: *nombre, apellidos, DNI, datos relativos al puesto de trabajo (departamento, categoría, turno, etc), correo electrónico, y número de teléfono asignado al usuario que previamente le hubiere asignado el Responsable del tratamiento.*

IV.- Fichaje App Móvil Geogestión con geolocalización: *nombre, apellidos, DNI, datos relativos al puesto de trabajo (departamento, categoría, turno, etc), correo electrónico, los datos del dispositivo móvil (código alfanumérico id único que se genera por la combinación del dispositivo y la aplicación Geogestión Horaria),y su geolocalización detallando las coordenadas de la ubicación del usuario, que solo se activará y recabará, en el momento en el que se realice el fichaje.*

V. IV.- Fichaje App Móvil Geogestión sin geolocalización: *nombre, apellidos, DNI, datos relativos al puesto de trabajo (departamento, categoría, turno, etc), correo electrónico, los datos del dispositivo móvil (código alfanumérico id único que se genera por la combinación del dispositivo y la aplicación Geogestión Horaria),*

VI.- Fichaje mediante enlace web: nombre, apellidos, DNI, datos relativos al puesto de trabajo (departamento, categoría, turno, etc), correo electrónico, código numérico asociado a un identificador único universal del equipo, asignado al usuario y en su caso, la Ip pública asociada y asignada por el Responsable del Tratamiento".

En conclusión, de la cronología expuesta se desprende que la implantación por el Ayuntamiento del nuevo sistema de control de horario denominado TARA para servir como medio de control de presencia de sus empleados públicosse realizó de forma progresiva, puesto que éste decidió ampliar las modalidades de fichaje de jornada escogidas, por lo que cambió el contrato de encargo inicial, y fue implantando las diversas modalidades por fases a medida que fue aprobando las normas municipales que eran legalmente precisas para poder convertir a dichos sistemas en medios de control de presencia obligatoria de su personal. Así pues:

- El 2-3-20 el Ayuntamiento contrata primeramente con el encargado del tratamiento MHP un sistema de control de horario que permitía el tratamiento de datos biométricos basados en huella dactilar y datos personales de localización, entre otros, pero no preveía la posibilidad de reconocimiento facial, suscribiendo un contrato preliminar de encargo que no concretaba las modalidades posibles de fichaje de jornada.

- Posteriormente, el Ayuntamiento decide ampliar el tratamiento al sistema de fichaje por reconocimiento facial, para lo que suscribe un nuevo contrato de encargo de 2-8-21 que concretaba 6 posibles modalidades de fichaje de la jornada, con los datos personales requeridos: fichaje biométrico mediante huella dactilar/reconocimiento facial, fichaje telefónico, fichaje App Móvil Geogestión con geolocalización, fichaje App Móvil Geogestión sin geolocalización, y Fichaje mediante enlace web. Y para ponerlos en marcha con fecha de 10-1-21 dicta una Circular en la que insta a sus empleados para quea partir de 2-11-21, comiencen a fichar mediante reconocimiento facial en los terminales de sus dependencias, y habilita excepcionalmente el fichaje mediante la conexión a través de sus ordenadores para casos de teletrabajo. Así pues, desde el 2-11-21 hasta que se aprueba y entra en vigor el Reglamento de Control de horario, las modalidades de fichaje fueron: a) sistema común: fichaje biométrico mediante reconocimiento facial, y b) sistema excepcional: fichaje mediante conexión vía web.

- Con la entrada en vigor del citado Reglamento de Control de Horario el 6-4-22, el Ayuntamiento amplió a 3 los sistemas de fichaje de la jornada, que comenzarían a ser obligatorios desde entonces hasta la actualidad para los empleados municipales, señalando en artículo 11 del Reglamento que "*sin perjuicio de la utilización de cualquier otro método, procedimiento o sistema de control de*

permanencia que se pudiera establecer, a los efectos del presente reglamento se podrán utilizar para el fichaje electrónico los siguientes medios y sistemas:
a) El Reconocimiento Facial.
b) Mediante Internet, a través de la web habilitada al efecto
c) El reconocimiento mediante la geolocalización.

2.2. Datos personales objeto de tratamiento.

El RGPD tiene por objeto garantizar el derecho a la protección de los datos de las personas físicas. El artículo 4.1 del RGPD entiende por "datos personales" "*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;".*

En el presente supuesto, estamos ante la implantación progresiva de un nuevo sistema de control de horario, denominado *Servicio Integral de la Gestión de Horarios TARA, en adelante, TARA)*, que afectó al tratamiento los datos personales de todos aquellos empleados municipales del Ayuntamiento obligados a utilizar los sistemas de fichaje que fueron fijados por el Ayuntamiento de Telde como medio de control de la jornada laboral.

Por lo que respecta a fijar las obligaciones en materia de tratamiento de datos personales, deben diferenciarse claramente dos momentos en dicha implantación progresiva:

- La implantación del nuevo sistema TARA comienza a partir del 2/11/2021, con carácter obligatorio, por orden de la Circular de 10-1-21 que instaba a fichar a través de reconocimiento facial en los terminales de las instalaciones para aquellos que prestaban una jornada presencial, y por conexión vía web para los que estaban excepcionalmente en jornada de teletrabajo.

- Y a partir de la entrada en vigor del Reglamento de control de horario el 6-4-22 (fecha de publicación en BOP), se ampliarían a 3 los sistemas de fichaje posibles: reconocimiento facial, fichaje conexión vía web, y fichaje a través de APP en el teléfono móvil con geolocalización.

Todos los datos que el Ayuntamiento debía poner a disposición para el funcionamiento de cada uno de los métodos de fichaje, según la cláusula segunda del contrato de encargo del tratamiento, revisten, sin lugar a dudas, el carácter de datos personales, en el sentido expresado en el artículo 4.1 del RGPD, toda vez que proporcionan "*información sobre una persona física identificada o identificable".* Lo que implica la obligatoriedad de aplicar la normativa de protección de datos a su tratamiento.

Entre estos datos personales, se encuentran datos personales de carácter identificativo propios de todos los sistemas de fichaje de control de jornada (*nombre, apellidos, DNI, datos relativos al puesto de trabajo (departamento, categoría, turno, código numérico asociado a un identificador único universal del equipo, asignado al usuario, correo electrónico del usuario, los datos del dispositivo móvil (código alfanumérico id único que*

se genera por la combinación del dispositivo y la aplicación Geogestión Horaria)), cuyo tratamiento está sometido a los principios y deberes previstos por la normativa de protección de datos con carácter general.

Pero los datos personales requeridos para llevar a cabo las operaciones de tratamiento que supone la implantación de los sistemas denominados como "fichaje biométrico" y "fichaje App Móvil Geogestión con geolocalización", tratan datos personales biométricos o de localización. Y el tratamiento de estos datos dentro de la finalidad de control de horario del personal, llevan aparejados consigo riesgos especialmente relevantes para los derechos y libertades de las personas, cuyo tratamiento va ligado al cumplimiento de **obligaciones específicas fijadas por el RGPD,** que se adicionan al cumplimiento de los principios y obligaciones fijados para el tratamiento de datos personales con carácter general.

- Así pues, por una parte, lo que el contrato denomina como "*minucia huella/patrón facial con su código numérico asociado*" utilizada para el fichaje biométrico tiene carácter de dato biométrico de carácter personal cuando se utiliza para identificar o autenticar la identidad de una persona de acuerdo con el artículo 4.14 del RGPD, como es el caso.

  Por tanto, si se pretende tratar datos biométricos para el control de la jornada laboral se tendrá que tener en cuenta: (i) que el dato biométrico es un dato personal de categoría especial, cuyo tratamiento está generalmente prohibido por el artículo 9.1 del RGPD, salvo que concurran ciertos supuestos excepcionales previstos en el artículo 9.2 del RGPD, cuya existencia deberá acreditarse para poder iniciar este tipo de tratamiento; (ii) y que el tratamiento de datos biométricos está considerado como "de alto riesgo" según el artículo 35 del RGPD, por lo que será necesario elaborar y superar una Evaluación de Impacto de Protección de Datos (en adelante, EIPD) que incluya todos estos elementos.

- Y por otra parte, cabe señalar que el sistema de fichaje mediante APP en el móvil con geolocalización implantado por el Ayuntamiento requiere tratar datos de "*geolocalización detallando las coordenadas de la ubicación del usuario",* son también datos de carácter personal, cuyo tratamiento es un asunto especialmente sensible por afectar a la libertad de circulación de las personas físicas, entrañando un alto riesgo para los derechos y libertades de los empleados que utiliza este método de fichaje de jornada, por lo que el RGPD requiere, también, la previa realización y superación de una EIPD, que se supervise de forma continua de acuerdo con lo exigido por el artículo 35 del RGPD.

2.3. Operaciones objeto de tratamiento.

El artículo 4.2 del RGPD define el "*tratamiento*" como "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;".*

De acuerdo con lo expuesto, la implantación del sistema de control de jornada laboral por el Ayuntamiento supuso la realización de un tratamiento de datos personales cuya finalidad es posibilitar el control de la jornada laboral de los empleados municipales del

Ayuntamiento, que está compuesto de 3 operaciones de tratamiento sobre un conjunto de datos personales diferentes, según el artículo 4.2 del RGPD:

A) Operaciones de tratamiento en relación con la finalidad de control de jornada mediante un sistema de reconocimiento facial, en el que se tratan, entre otros, los datos personales biométricos.
B) Operaciones de tratamiento en relación con la finalidad de control de jornada mediante un sistema geolocalización, en el que se tratan, entre otros, los datos personales de localización que requiere la conexión mediante geolocalización a través de una APP en el móvil.
C) Operaciones de tratamiento en relación con la finalidad de control de jornada mediante un sistema de conexión web respecto de los datos personales que se requieren para el sistema de fichaje mediante conexión vía web.

En conclusión, la implantación del nuevo sistema de gestión de horario denominado TARA supuso el inició de un nuevo tratamiento de control de horario por el Ayuntamiento, compuesto de 3 operaciones de tratamiento (una por cada sistema de fichaje), que encaja en el concepto previsto en el artículo 4.2 del RGPD. Tratamiento respecto del que son aplicables todos los principios y obligaciones exigidos en la normativa de protección de datos personales.

2. 4. Responsable del tratamiento.

Por lo que respecta a la responsabilidad, el artículo 4. 7 del RGPD, define al: **"***7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".*

Tal y como se ha expuesto, consta acreditado que el Ayuntamiento contrató a la entidad MHP como encargada del tratamiento. No obstante, del examen de las normas municipales y contrato de encargo aportados al procedimiento se deducen múltiples evidencias que confirman que el Ayuntamiento es el responsable del tratamiento, pues es el que define los fines y medios del tratamiento, a los efectos previstos en el artículo 4.7 del RGPD:

- De la suscripción de los dos contratos de encargo del tratamiento de 2020 y 2021 entre Ayuntamiento y MHP. En ambos documentos contractuales la cláusula cuarta define las obligaciones del "responsable del tratamiento" y "encargado del tratamiento". Y se contiene una cláusula primera que señalan lo siguiente: "*PRIMERO.- Objeto y finalidad del presente contrato de Encargo del Tratamiento", en cuyo párrafo segundo se hace constar que: "Sea como fuere, el tratamiento de los datos por parte del Encargado del Tratamiento, se limitará a las actuaciones necesarias para desarrollar correctamente el servicio, siguiendo las instrucciones documentadas que, en cada caso, le dirija el Responsable del Tratamiento, tal y como exige el vigente Reglamento Europeo (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, en adelante RGPD y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)".*

- La Circular de la Concejalía de Recursos Humanos de 10/01/21 insta por primera vez a los empleados municipales a fichar conforme al nuevo sistema que se aprobaría por Reglamento del pleno posteriormente, lo que acredita que fue el Ayuntamiento el que fijó las modalidades de fichaje de jornada a las que los empleados estarían obligados, y los datos personales que deberán ser objeto de tratamiento en cada uno.

- De la aprobación del Reglamento de jornada laboral de 31/03/21 (en vigor desde el 6/4/22), que señala en su artículo 3, las siguientes normas aplicables en materia de tratamiento de datos personales: "*Artículo 3.-Tratamiento de los datos personales 1. Cualquier sistema que se utilice para el control horario o control y gestión de los permisos ylicencias, deberá adecuarse a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y al Reglamento (UE) 2016/679 del ParlamentoEuropeo y Consejo de 27 de abril de 2016. 2. El Ayuntamiento de deberá informar de forma expresa, clara e inequívoca a los trabajadores/as, acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión. 3. Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación a losfines para los que son tratados (minimización de datos), exactos y si fuera necesario actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan".*

En conclusión, podríamos decir que del contenido de ambos contratos se desprende claramente que es el Ayuntamiento el que fija los medios y fines del tratamiento, y que MHP debe seguir sus instrucciones. Así pues,es el Ayuntamiento el que fija las instrucciones de los diferentes sistemas de fichaje que el encargado debe cumplir y desarrollar, proporciona los datos personales de sus empleados (incluidos los biométricos) al encargado, y es el que debe adoptar las medidas técnicas y organizativas del artículo 24 y 32 del RGPD.

En definitiva, solo el Ayuntamiento de Telde es responsable del tratamiento de los datos personales que se realizó con la finalidad de controlar el horario de la jornada laboral de sus empleados. En consecuencia, es el Ayuntamiento el presunto responsable frente al que debe dirigirse el presente procedimiento sancionador en caso de cometer alguno de los incumplimientos tipificados como infracción, de acuerdo con lo previsto en el artículo 70. 1 a) de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales (en adelante, LOPPDD):

"Artículo 70. Sujetos responsables.

1. *Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica: a) Los responsables de los tratamientos. b) Los encargados de los tratamientos. c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea. d) Las entidades de certificación. e) Las entidades acreditadas de supervisión de los códigos de conducta. (…)".*

III. Sobre la obligación de realiza y superar una EIPD del artículo 35 del RGPD

3.1. Sobre los riesgos derivados del tratamiento de datos personales biométricos y datos personales de localización.

De acuerdo con el Principio de Gestión de Riesgos desde el diseño y por defecto, así como el Principio de Responsabilidad Proactiva, inspiradores de la nueva regulación, el nuevo RGPD hace hincapié en que el responsable debe evaluar seriamente los riesgos del tratamiento que quiera establecer en los derechos y libertades de los interesados (siempre previamente a iniciar cualquier tratamiento, y de forma continua si decide hacerlo), optando por un enfoque de análisis de riesgos desde el diseño y por defecto, para poder identificarlos, determinar la probabilidad de materialización y su impacto y prever medidas y garantías que eliminen o, cuando menos, mitiguen los riesgos detectados, evitando su materialización. Análisis que el responsable debe documentar, e incluir en una preceptiva EIPD en el caso de que sea probable que el tratamiento entrañe un “alto riesgo” de acuerdo con lo previsto en el artículo 35 del RGPD.

Este previo análisis de riesgos es especialmente importante cuando el tratamiento de datos personales lo realizan las Administraciones Públicas (en adelante, AA.PP), ya que como señala la Guía de Tecnologías y protección de datos en las AA.PP publicada por esta Agencia Española de Protección de Datos:

> **“***El tratamiento de datos personales en las AA.PP. implica riesgos distintos frente a los riesgos de un tratamiento que pueda realizar cualquier otro responsable y que se derivan, al menos, del volumen de sujetos afectados, de la extensión de los datos recogidos, de la imposibilidad, en muchos casos, de oponerse al tratamiento y del poder o asimetría inherente que existe entre las AA.PP. y los ciudadanos o interesados de los que tratan datos. Por otra parte, independientemente del hecho de que todos los tratamientos en las AA.PP. están guiados por un espíritu de servicio público, el mismo que alienta el trabajo de sus empleados, estos posibles riesgos podrían materializarse sobre los ciudadanos en determinadas situaciones, como, por ejemplo, situaciones de quiebras del estado de derecho, situaciones de abuso por parte de los responsables públicos, en circunstancias de filtrado masivo o selectivo de datos personales como consecuencia de brechas de seguridad, ante supuestos de posibles cambios legislativos incluso en terceros países a los que hubieran sido transferidos los datos, ante casos de corrupción, en situaciones de emergencia fuera de control,… etc”.*

En consecuencia, las AA.PP., en tanto que son responsables del tratamiento de los datos de los ciudadanos, antes de poner en marcha nuevas actividades de tratamiento o modificar servicios ya prestados que hagan uso de tecnologías que no hayan utilizado con anterioridad, siendo la primera ocasión que las implementan para una determinada finalidad, deberán identificar aquellos riesgos a los que pueda estar expuesto el tratamiento. También deberán adoptar las medidas técnicas y organizativas necesarias que, desde el diseño y por defecto, permitan eliminar o al menos mitigar a un nivel aceptable, los riesgos que, para los derechos y libertades de las personas, pudieran derivarse del tratamiento.

La decisión de optar por un tratamiento basado en métodos biométricos como la huella dactilar o el reconocimiento facial o métodos que traten datos de localización de las personas físicas no es baladí. Este tratamiento puede ser realmente intrusivo y requiere

de un debate ético y jurídico sosegado antes de decidir su implantación, toda vez que recoger la huella dactilar, sacar un patrón/vector facial o recoger las coordenadas de localización del personal puede tener efectos muy adversos en los derechos fundamentales y la libertad e integridad humana de estos empleados que no se producen con otros métodos de control de jornada.

Véanse solo alguna de las características especiales de los sistemas de identificación unívoca basados en **datos biométricos** y piénsese en impacto significativo que producen cuando se comprometen estos datos, en comparación a otros métodos (firma y cumplimentación de hojas, tarjetas magnéticas…etc):

- Los datos biométricos pueden tratarse y almacenarse de diferentes formas. A veces, la información biométrica capturada de una persona se almacena y se trata en bruto, lo que permite reconocer la fuente de la que procede sin conocimientos especiales; por ejemplo, la fotografía de una cara, la fotografía de una huella dactilar o una grabación de voz. Otras veces, la información biométrica bruta capturada es tratada de manera que solo se extraen ciertas características o rasgos y se salvan como una plantilla biométrica, aquí llamado "*minucia dactilar*" para la huella; y "*patrón facial*" para el reconocimiento facial.
- A diferencia de otros datos personales, los datos biométricos son únicos, permanentes o definitivos en el tiempo y la persona no puede liberarse de ellos, no se pueden cambiar nunca, ni con la edad, por lo que el daño creado en caso de compromiso-pérdida o intrusión en el sistema es irreparable en este caso. A diferencia de una contraseña, en caso de pérdida, los datos de nuestra huella dactilar o cara no se pueden cambiar.
- Además, debido a que los datos biométricos son propios de una persona y perpetuos, el usuario puede utilizar los mismos datos en diferentes sistemas, lo que supone un riesgo extra.
- Mientras que los métodos tradicionales de autenticación como las contraseñas requieren una coincidencia del 100% de carácter por carácter para permitir que el usuario acceda por ejemplo a una cuenta o aplicación (métodos deterministas), los métodos de biometría se denominan "*probabilísticos*", porque se basan en la probabilidad de que el usuario que intenta acceder a un determinado dispositivo o aplicación sea la misma persona que el usuario registrado. Podemos medir el rendimiento de un sistema biométrico a partir de tres características principales. Estas son: tasa de falsos rechazos (FRR), tasa de falsas aceptaciones (FAR) y tasa de errores iguales (ERR). La tasa de falsos rechazos representa la probabilidad de errores de detección por parte de un sistema biométrico, lo que significa que no puede reconocer a un usuario cuyas características biométricas ya están en la base de datos. En caso de rechazo, la persona debe verificar su identidad de nuevo. Desde una perspectiva de seguridad y protección, esta tasa no significa que sea necesariamente un resultado negativo. Cada método biométrico, ya sea lectura de cara, de huella dactilar, huella palmar, iris, etc., tiene diferentes valores para diferentes tasas en función de las cuales un sistema rechaza o acepta las entradas. Tasas de errores que por lo que manifiesta el Ayuntamiento fueron altas en este caso.

Cabe destacar, además, que dentro de los métodos que utilizan datos biométricos, los basados en reconocimiento facial (implantado como sistema general de fichaje de jornada por el Ayuntamiento) pueden ser incluso más intrusivos que los de detección de huella dactilar, incrementando exponencialmente los riesgos para los derechos y libertades fundamentales de los interesados, dados los usos que tiene el reconocimiento facial, máxime cuando se suma a la inteligencia artificial como sistema de reconocimiento automatizado de rasgos humanos.

Así lo han puesto de manifiesto las Directrices 05/2022 del Consejo Europeo de Protección de Datos (en adelante, CEPD) sobre el uso de la tecnología de reconocimiento facial (denominada FRT) en el ámbito de aplicación de la ley, órgano consultivo independiente y máxima autoridad en la materia, que indica lo siguiente (el subrayado es nuestro):

> "*Gran parte del mayor interés en FRT se basa en la eficiencia y escalabilidad de FRT. Con estos vienen las desventajas inherentes a la tecnología y su aplicación, también a gran escala. Si bien puede haber miles de conjuntos de datos personales analizados con solo pulsar un botón, los efectos ya leves de la discriminación algorítmica o la identificación errónea pueden crear un gran número de personas afectadas severamente en su conducta y en su vida diaria. El gran tamaño del tratamiento de los datos personales, y en particular de los datos biométricos, es posible otro elemento clave del FRT, ya que el tratamiento de datos personales constituye una injerencia en el derecho fundamental a la protección de los datos personales de conformidad con el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «la Carta»).*
> *La aplicación de la FRT de las LEA tendrá, y en cierta medida ya lo hace, importantes implicaciones para las personas y los grupos de personas, incluidas las minorías. Estas implicaciones también tendrán efectos considerables en la forma en que vivimos juntos y en nuestra estabilidad política social y democrática, valorando la gran importancia del pluralismo y la oposición política. El derecho a la protección de los datos personales a menudo es clave como requisito previo para garantizar otros derechos fundamentales. La aplicación de FRT es considerablemente propensa a interferir con los derechos fundamentales más allá del derecho a la protección de datos personales".*
>
> *En este contexto, el CEPD considera importante recordar que el FRT, ya sea para fines de autenticación o identificación, no prevé un resultado definitivo, sino que se basa en probabilidades de que dos caras, o imágenes de caras, correspondan a la misma persona. Este resultado se degrada aún más cuando la calidad de la entrada de muestra biométrica al reconocimiento facial es baja. La borrosidad de las imágenes de entrada, la baja resolución de la cámara, el movimiento y la poca luz, pueden ser factores de baja calidad. Otros aspectos con un impacto significativo en los resultados son la prevalencia y la falsificación, por ejemplo, cuando los delincuentes intentan evitar pasar por las cámaras o engañar a la FRT. Numerosos estudios también han puesto de relieve que tales resultados estadísticos del procesamiento algorítmico también pueden estar sujetos a sesgos, en particular como resultado de la calidad de los datos de origen, así como de las bases de datos de capacitación u otros factores, como la elección de la ubicación del despliegue. Además, cabe destacar el impacto de la tecnología de reconocimiento facial en otros derechos fundamentales, como el respeto de la vida privada y familiar, la libertad de expresión e información, la libertad de reunión y asociación, etc (…)*"

Algo similar sucede cuando tratamos **datos personales de localización** de las personas físicas, utilizando métodos de geolocalización que se implantan en dispositivos móviles, como los que precisa el sistema de fichaje a través de APP móvil con geolocalización utilizado por el Ayuntamiento.

Esta opción tiene consecuencias que afectan e incluso trascienden al ámbito de la protección de datos personales, dado que, de acuerdo con lo que ya fue señalado en el Dictamen 5/2005 del Grupo de Trabajo del Artículo 29, predecesor del actual CEPD: *"el tratamiento de los datos de localización o coordenadas es un asunto especialmente sensible por referirse a la cuestión esencial de la libre de circulación de las personas de forma anónima*", que puede afectar gravemente, no sólo a la protección de datos personales, sino también a otros derechos fundamentales y libertades de las personas físicas que son geolocalizadas a través de ellos.

El artículo 2 de la Directiva 2002/58/CE define los datos de localización *como "cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público".*

El CEPD ya venía advirtiendo del grave riesgo que implica la utilización de infraestructuras que emplean geolocalización, incluso desde antes de la aprobación del nuevo RGPD. En especial, destaca el *Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes, adoptado el 16 de mayo de 2011*, que analizaba los riesgos que supone la utilización de 3 tipos de infraestructuras que emplean geolocalización (Wifi, estaciones base, y tecnología GPS), indicando lo siguiente (el subrayado es nuestro):

> *"Los dispositivos móviles inteligentes están muy estrechamente vinculados a las personas porque la mayoría de ellas tienden a mantener su dispositivo móvil muy cerca de ellas, en el bolsillo, en el bolso o sobre la mesilla de noche. Raramente ocurre que una persona preste su dispositivo a otra. (…)*
> *Esto permite a los proveedores de servicios de geolocalización disponer de una panorámica detallada de los hábitos y pautas del propietario de estos dispositivos y establecer unos perfiles exhaustivos. A partir de un período de inactividad nocturna puede deducirse el lugar donde duerme la persona, y a partir de una pauta de desplazamientos regulares por la mañana, la localización de su empresa. El perfil puede incluir asimismo datos derivados de las pautas de movimientos de sus amigos, sobre la base de lo que se conoce como «gráfica social»*
> *Un modelo de comportamiento también podría incluir categorías especiales de datos,*
> *por ejemplo visitas a hospitales y lugares de culto, presencia en actos políticos o en otros lugares específicos que, verbigracia, revelen datos sobre la vida sexual. Estos. perfiles pueden ser utilizados para tomar decisiones que afecten significativamente a su propietario.*
> *La tecnología de los dispositivos móviles inteligentes permite un control constante de los datos de localización. Los teléfonos inteligentes pueden captar permanentemente las señales procedentes de las estaciones de base y de puntos de acceso WiFi. Técnicamente, el seguimiento puede hacerse de forma secreta, sin informar al propietario, o también de forma semisecreta, cuando la persona «olvida» o no está adecuadamente informada de que los servicios de localización están activados o cuando los parámetros de accesibilidad de los datos sobre localización son cambiados de «privada» a «pública».*
> *Aun cuando las personas permitan deliberadamente el acceso a sus datos de geolocalización en Internet, mediante servicios de rastreo y etiquetado geográfico, un acceso general e ilimitado crea nuevos riesgos que van desde la sustracción de datos hasta los robos en domicilios o incluso agresiones físicas y acoso. Como ocurre con otras nuevas tecnologías, un riesgo importante del uso de datos de*

localización es la desviación de uso, el hecho de que, sobre la base de la disponibilidad de un nuevo tipo de datos, se desarrollen nuevos fines no previstos en el momento de la recogida de los datos."

El Dictamen 2017 WP 249 del Grupo de Trabajo 29 de 8 de junio de 2017 sobre tratamiento datos personales en el trabajo, que regula las operaciones de tratamiento derivadas de la observación del uso de las TIC fuera del lugar de trabajo, pone de manifiesto los riesgos "añadidos" que presentan el tratamiento de datos personales de localización cuando el empleador utiliza dispositivos móviles del propio empleado, o procesos de administración de dispositivos móviles (los denominados MDM), como es el caso de la APP de fichaje a la que se refiere ese expediente. En ambos casos, el tratamiento tiende a extenderse a la esfera doméstica de los empleados, por lo que son necesarios ciertos límites.

En concreto, los puntos 5.4.2 y 5.4.3 del Dictamen 2017 W 249 se refieren a la problemática planteada en el supuesto presente, en que el Ayuntamiento atendió las peticiones de sus empleados, que se prestaron voluntarios para utilizar el sistema de fichaje en el móvil mediante la instalación de una APP con geolocalización en su dispositivo personal. Nótese, que el GT 29 ya señalaba en el año 2017 expresamente que será necesario realizar una EIPD antes de utilizar estas tecnologías, al menos cuando esta tecnología sea nueva o desconocida para el responsable.

"5.4.2 UTILIZACIÓN DEL PROPIO DISPOSITIVO DEL TRABAJADOR
Debido al aumento de la popularidad, las funcionalidades y la capacidad de los dispositivos electrónicos de consumo, los empresarios pueden enfrentarse a peticiones de los trabajadores de utilizar sus propios dispositivos en el lugar de trabajo para llevar a cabo sus tareas. (…) Sin embargo, el uso del dispositivo de un trabajador será personal por naturaleza, y esto es más probable que ocurra en ciertos momentos del día (por ejemplo, por la noche y los fines de semana). Por tanto, es posible que el uso de sus propios dispositivos por parte de los trabajadores conduzca a que los empresarios traten información extraempresarial sobre ellos y, posiblemente, sobre cualquier miembro de la familia que también utilice los dispositivos. (…)

5.4.3 GESTIÓN DE DISPOSITIVOS MÓVILES (MDM)
La gestión de dispositivos móviles permite a los empresarios localizar dispositivos de forma remota, utilizar configuraciones y/o aplicaciones específicas y borrar datos previa petición. Un empresario puede gestionar esta funcionalidad por sí mismo, o utilizar a un tercero para hacerlo. Los servicios de MDM también permiten que los empresarios registren o sigan el dispositivo instantáneamente, incluso si no se ha denunciado su robo.

Debe realizarse una EIPD antes de utilizar cualquier tecnología de este tipo cuando para el responsable del tratamiento sea nueva o desconocida. Si el resultado de la EIPD es que la tecnología MDM es necesaria en circunstancias específicas, aún debe evaluarse si el tratamiento de datos resultante cumple los principios de proporcionalidad y subsidiariedad. Los empresarios deben asegurarse de que los datos recogidos como parte de esta capacidad de

localización remota se traten con un fin específico y no formen parte de un programa más amplio que permita la observación continua de los trabajadores. Incluso para los fines especificados, las funciones de seguimiento deben mitigarse. Los sistemas de seguimiento se pueden diseñar para registrar los datos de localización sin presentarlos al empresario. En tales circunstancias, los datos de localización deben estar disponibles únicamente cuando el dispositivo sea objeto de denuncia o se pierda.
Los trabajadores cuyos dispositivos estén inscritos en los servicios de MDM también deben ser plenamente informados sobre el seguimiento llevado a cabo y las consecuencias que esto tiene para ellos."

3.2. Sobre la necesidad de realizar y superar una EIPD.

La evaluación de impacto en la protección de datos personales, EIPD, aparece como la herramienta exigida por el RGPD para garantizar que se cumple con esta vertiente cuando el tratamiento se considerado de "alto riesgo", según lo establecido en el artículo 35 en su apartado1 del RGPD (el subrayado es nuestro):

"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…"

Esta evaluación se hará con carácter previo al inicio del tratamiento, pero deberá entenderse como una evaluación continua o periódica, en el sentido establecido por el artículo 35.11 del RGPD, que dispone*: "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.*"

Una EIPD debe cumplir con los requisitos o contenido mínimo relacionado en el artículo 35.7 del RGPD, que dispone:

"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".

En definitiva, la superación de una EIPD exige que el responsable de un tratamiento de alto riesgo documente por escrito que supera la evaluación de idoneidad, necesidad y proporcionalidad del tratamiento, y que gestione desde el diseño los riesgos específicos del tratamiento, con la aplicación práctica de medidas orientadas a los mismos de forma que se garantice un umbral de riesgo aceptable durante todo el ciclo de vida del tratamiento, tal como se establece en el artículo 35 del RGPD.

Además, obliga a la consulta previa a la autoridad de control en caso de que el responsable no haya tomado medidas que permitan mitigar el riesgo de acuerdo al artículo 36 del RGPD.

En el presente supuesto, no cabe duda de que era obligatorio realizar y superar una previa EIPD, dado que era y es probable que el tratamiento de control de horario que implantó el Ayuntamiento entrañase un alto riesgo para los derechos y libertades de los empleados públicos que utilizasen los sistemas de fichaje biométrico y de fichaje a través de APP en el móvil con geolocalización, vista su naturaleza, alcance, contexto y fines, tal y como determina el artículo 35.1 del RGPD.

Tal y como se ha expuesto, el tratamiento de los datos personales biométricos y los datos personales de localización en el ámbito de control de la jornada laboral lleva aparejados riesgos relevantes y especialmente significativos para los derechos y libertades de las personas cuyo tratamiento ya entraña, por sí solos y por separado, una probabilidad de alto riesgo para los derechos y libertades de los empleados merecedora de una EIPD, previa y válida. Y en este supuesto, en el que se optó por tratar ambos tipos de datos y asumir el alto riesgo que ambos conllevan, la calificación de alto riesgo del tratamiento es innegable.

A mayor abundamiento, hay que señalar que datos biométricos dirigidos a la identificación-autenticación de las personas -como es el caso de estos sistemas de fichaje para control de la jornada laboral-, han sido expresamente incluidos en la Lista de tipos de tratamiento de datos que requieren evaluación de impacto relativa a la protección de datos, publicada por la AEPD el 6 de mayo de 2019, en desarrollo de la previsión contemplada en el apartado cuarto del referido artículo 35 del RGPD, que prevé que las autoridades de control establezcan y publiquen listas que definan los tratamientos que requieran EIPD.

En el caso del estado español, se ha optado por publicar una lista no exhaustiva, en la que se determina que "*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" (*criterios 4 y 5 en el caso de los datos biométricos para control de jornada o asistencia). No obstante, ello no excluye a otros tratamientos que no cumplan con estos criterios, pero a la luz de su naturaleza, alcance, contexto y fines exista probabilidad de que entrañen un alto riesgo a los efectos previstos en el artículo 35.1 del RGPD, tal y como sucede con el tratamiento de los datos de localización que son necesarios para arbitrar el sistema de fichaje de la jornada laboral a través de APP en el móvil con geolocalización.

En el presente supuesto, el Ayuntamiento ha reconocido que no realizó una EIPD, ni previa, ni durante, ni posteriormente al inicio del nuevo tratamiento de control de horario implantado, en sus diferentes fases. Y no ha presentado alegaciones al acuerdo de inicio, que manifiesten o acrediten lo contrario.

En relación con el documento 8 acompañado por MHP, que aporta un Protocolo de Implantación del sistema TARA, edición revisada a octubre de 2022, que de acuerdo con su apartado 1, se ofrece a los clientes del sistema TARA a nivel orientativo, en cuyo apartado 13 "Modelos sugeridos*: 13.4 Evaluación de Impacto por parte del Responsable del Tratamiento"* acompaña una propuesta de EIPD cabe aclarar que el mismo no constituye una EIPD válida, toda vez que no ha sido elaborada y firmada por el responsable del tratamiento, que es el obligado a realizarla y superarla, y tampoco consta acreditación de que dicho protocolo se entregase al Ayuntamiento, en el supuesto presente. Se trata de un mero modelo sugerido por MHP, sin validez ni efectos jurídicos, que tampoco dispone de fecha ni firma de dicha entidad, en la que se

hace constar la siguiente leyenda: *"El presente documento ha sido elaborado por el departamento jurídico de MHP, solamente a efectos orientativos y de conformidad con la normativa que resultare de aplicación a 4 de marzo de 2021".* Por tanto, dicho documento no puede ser tenido en cuenta a los efectos de cumplir con la obligación del artículo 35 del RGPD.

3.3. Sobre la exigencia de que el tratamiento sea necesario, idóneo y proporcional.

No haber realizado y superado la preceptiva EIPD en este supuesto supone, entre otras cosas, que el Ayuntamiento inició las operaciones de tratamiento del nuevo sistema de control de horario sin realizar previamente el juicio sobre su necesidad, idoneidad y proporcionalidad al que le obligan los artículos 5.1.c) y 35.4.b) del RGPD.

Así pues, el artículo 5.1.c) del RGPD, recoge el denominado "Principio de minimización de datos personales" que dispone lo siguiente:

> "1*. Los datos personales serán:*
> a) *adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)".*

El respeto de este principio deberá ser el punto de partida del inicio de todo tratamiento, debiendo plantearse el responsable si este tratamiento será realmente necesario, idóneo, y proporcional antes de iniciarlo. Por tanto, este previo análisis debe realizarse antes del inicio de cualquier tratamiento de datos personales, si bien cuando existe probabilidad de que el tratamiento entrañe un alto riesgo (como es el caso de los biométricos y datos de localización tratados en este sistema de fichaje de control de jornada) existe obligación de documentarlo dentro de la EIPD, toda vez que ésta debe contener "*b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad",* de acuerdo con el artículo 35.7. b) del RGPD.

Ello se confirma por el considerando 39 del RGPD, que subraya la importancia de que el tratamiento sea necesario, indicando que *"Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios*."

En la misma línea se pronuncia el Grupo de Trabajo del artículo 29, en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas.

La obligación de tratar únicamente "*los datos personales que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"* prevista por el principio de minimización de datos~~/~~ del artículo 5.1.c) del RGPD, y de evaluar la necesidad y proporcionalidad del tratamiento en la EIPD según el artículo 35.7 b) del RGPD, debe interpretarse de conformidad con lo previsto por la reiterada jurisprudencia de nuestro Tribunal Constitucional respecto a la necesidad de constatar que toda medida restrictiva de derechos fundamentales (operaciones de tratamiento que comprenden datos biométricos y de geolocalización en este caso) supera lo que se denomina como "el triple juicio de proporcionalidad".

Ello implica que, antes que nada, es necesario constatar si cumple los tres siguientes requisitos o condiciones a los que se refiere el Tribunal Constitucional: *«si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la*

misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)".

La exigencia de realizar este triple juicio de proporcionalidad previo al tratamiento se especifica en lo que respecta a datos biométricos en el apartado 72*,* de las Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo, de 29/01/2020, del CEPD, que indica*: "El uso de datos biométricos y, en particular, del reconocimiento facial conllevan elevados riesgos para los derechos de los interesados. Es fundamental que el recurso a dichas tecnologías tenga lugar respetando debidamente los principios de licitud, necesidad, proporcionalidad y minimización de datos tal y como establece el RGPD. Aunque la utilización de estas tecnologías se pueda percibir como particularmente eficaz, los responsables del tratamiento deben en primer lugar evaluar el impacto en los derechos y libertades fundamentales y considerar medios menos intrusivos de lograr su fin legítimo del tratamiento.* Es decir, habría que responder la cuestión de si esta aplicación biométrica es algo que realmente es imprescindible y necesaria, o es solo "*conveniente*".

Por lo que respecta a los datos de localización, el Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido del GT 29 del CEPD, previno ya, en el año 2005, que el tratamiento de estos datos para efectuar simplemente un control laboral de su jornada se considera "excesivo" a los efectos del Principio de minimización de datos: «*El tratamiento de los datos de localización puede estar justificado si se lleva a cabo formando parte del control del transporte de personas o bienes o de la mejora de la distribución de los recursos para servicios en puntos remotos (por ejemplo, la planificación de operaciones en tiempo real) o cuando se trate de lograr un objetivo de seguridad en relación con el propio empleado o con los bienes o vehículos a su cargo. Por el contrario, el Grupo considera que el tratamiento de datos es excesivo en el caso de que los empleados puedan organizar libremente sus planes de viaje o cuando se lleve a cabo con el único fin de controlar el trabajo de un empleado, siempre que pueda hacerse por otros medios».*

En el presente supuesto, no consta una evaluación de esta necesidad, idoneidad y proporcionalidad, dado que el Ayuntamiento no ha realizado la preceptiva EIPD. Y tampoco hay evidencias constatadas de que el Ayuntamiento analizase exhaustivamente y antes del tratamiento si las operaciones de tratamiento biométricos y de geolocalización a través de móvil eran realmente idóneos, necesarios y proporcionales para cumplir con la finalidad de control de cumplimiento de la jornada laboral de sus empleados. Lo que es requisito previo e inicial, sin el cual no cabe continuar con la EIPD, puesto que el tratamiento de aquellos datos personales que no sean necesarios, idóneos y proporcionales está prohibido por el RGPD.

Pero además de no haberse realizado dicho triple juicio previo de proporcionalidad, cabe advertir que no constan evidencias en el procedimiento de que los sistemas de fichaje biométrico y de geolocalización a través de una APP en el móvil fueran necesarios para cumplir con la finalidad de control de jornada laboral, para la que fueron implantados.

Ello es así dado que consta acreditado que existían y se podían utilizar otros sistemas de fichaje menos intrusivos que permitían cumplir con la finalidad pretendida con menores riesgos para los interesados, tales como el sistema de fichaje mediante internet a través de conexión vía web que está ya en funcionamiento (siempre y cuando éste no recoja datos de localización, sino los datos personales que se indican

en el contrato de encargo del tratamiento); u otros posibles como las tarjetas magnéticas u hojas de firmas que ya se habían utilizado con anterioridad por el Ayuntamiento y son de fácil implantación por el mismo.

No parece, por tanto, necesario ni proporcional, dada la relación entre ventajas y desventajas, utilizar sistemas de fichaje del horario de la jornada laboral que se basen en tratamientos de datos personales biométricos y de geolocalización, cuando existen otros posibles métodos alternativos de fichaje del horario igual de eficaces, por lo que difícilmente se superará esta evaluación o triple juicio de proporcionalidad en la EIPD.

En conclusión, de conformidad con los hechos probados, tras las actuaciones de investigación e instrucción practicada, se considera que los hechos expuestos podrían vulnerar lo establecido en el artículo 35 del RGPD*,* por no realizar y superar el Ayuntamiento una EIPD previa al inicio del tratamiento de control de horario que fue implantado.

IV. Tipificación y calificación de la infracción del artículo 35 del RGPD.

Tal y como se ha expuesto en el Fundamento de Derecho III, se considera que los hechos expuestos vulneran lo establecido en el artículo 35 del RGPD, lo que podría suponer la comisión de una infracción administrativa tipificada en el artículo 83.4.a) del RGPD que indica que:

> "*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*."

A los efectos de prescripción, la LOPDGDD establece en su artículo 73.t) que: "*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."*

V. Sobre la prohibición de tratar datos de categoría especial del artículo 9 del RGPD

5.1. Los datos biométricos como datos de categoría especial: prohibición general y excepciones de tratamiento.

El RGPD define el art.4.14 datos biométricos como "*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*".

De acuerdo con la definición dada por el artículo 4.14 del RGPD, los datos biométricos tratados por estos sistemas se convertirán en datos de carácter personal siempre y cuando la finalidad del tratamiento sea la identificación o autenticación de una persona, en el sentido previsto en el artículo 4.1 del RGPD.

No cabe duda de que las minucias (huellas dactilares) y el patrón facial que son necesarios para el fichaje biométrico previsto por el Ayuntamiento son datos biométricos de carácter personal, puesto que la finalidad del sistema implantado es determinar la identidad, directa o indirectamente, de los empleados municipales del Ayuntamiento reclamado, al objeto de registrar su entrada y salida del centro de trabajo, y comprobar la hora y fecha del comienzo y fin de su jornada laboral. Toda vez que el proceso asigna un identificador (la plantilla biométrica obtenida al recoger las muestras de huella dactilar o reconocimiento facial de los interesados) que permite singularizar a un individuo y, distinguirlo frente a otros, a través de “elementos propios de la identidad física, fisiológica, genética, psíquica”.

Se debe considerar además que -a diferencia de lo que sucedía bajo el régimen anterior al RGPD- este tipo de datos biométricos están considerados como **datos personales de categoría especial** en el artículo 9, cuyo tratamiento está generalmente prohibido, salvo que concurra alguna de las excepciones previstas en el artículo 9.2 del RGPD. Lo que no exime de que siempre deba existir además una base de licitud prevista en el artículo 6 del mismo, entre otros muchos requisitos y principios que deberá cumplir aquel que decida optar por este tipo de tratamientos.

De acuerdo con el artículo 9.1 del RGPD, queda prohibido el tratamiento de datos biométricos cuando sean: “*datos biométricos dirigidos a identificar de manera unívoca a una persona física*”.

En el caso concreto de las técnicas de reconocimiento facial (TRF), sistema general de fichaje que fue implantado por el Ayuntamiento, no cabe duda de que el “patrón facial” extraído de cada persona, permite identificarla de forma unívoca. El uso de la cara en las TRF es capaz de validar la identidad, conteniendo información única sobre las personas físicas. El algoritmo del software, sobre la muestra biométrica (fotografía de la cara de la persona), extrae las características biométricas de la cara de una persona a través de una fotografía, reduce y transforma en etiqueta o números esa muestra, constituyendo una representación matemática de la característica biométrica original, que es la plantilla biométrica (patrón o vector facial). La plantilla se almacena para su comparación en la última fase en la cual con la muestra biométrica- en el lector-y con la plantilla previamente grabada, está identificando unívocamente al usuario, en cada ocasión que entra poniendo su cara ante el lector, por lo que se considera que los datos entran dentro del ámbito de los datos especiales, por ser una identificación unívoca.

En este orden de cosas tenemos que, siendo los datos biométricos datos de categoría especial, el RGPD impone una obligación adicional al responsable del tratamiento de los mismos, que estará obligado también a comprobar y acreditar que concurre una de las excepciones previstas en el artículo 9.2 del RGPD u otra legislación específica, antes de iniciar el tratamiento de ningún dato biométrico, lo que se aplica al supuesto presente, en el que se previno el fichaje biométrico como método general de fichaje basado en el reconocimiento facial de los empleados.

Hay que señalar que, estando prohibido el tratamiento de datos biométricos con carácter general, cualquier excepción a dicha prohibición habrá de ser objeto de interpretación restrictiva, tal y como se deduce de los considerandos 51 y 52 del RGPD.

Así las cosas, las excepciones que posiblemente podrían permitir el levantamiento de la prohibición general de tratar datos biométricos dirigidos a identificar-verificar la identidad de personas físicas, son las que prevé el artículo 9.2. del RGPD, con el siguiente tenor literal, que deberá interpretarse restrictivamente, siempre en favor de proteger los derechos y libertades de los ciudadanos en caso de duda:

"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.*
c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;
i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

Por tanto, además de no haber realizado una EIPD válida, si el responsable no acredita que su tratamiento está dentro de alguna de estas excepciones, incurrirá en una infracción del artículo 9 del RGPD por iniciar un tratamiento prohibido.

5.2. Análisis del supuesto presente.

En el presente supuesto, consta acreditado en la instrucción que el Ayuntamiento ha tratado datos biométricos, implantando el sistema de huella dactilar desde 2015, y el de reconocimiento facial como sistema común de fichaje de la jornada laboral de sus empleados municipales desde 2/11/21.

Según lo expuesto, para que estos sistemas de fichaje biométrico sean conformes a derecho, es necesario que concurra una excepción a la prohibición general de tratamiento de datos de categoría especial prevista en el artículo 9.1. del RGPD, además de una base de licitud del artículo 6 del RGPD. No es cuestión discutida que el Ayuntamiento dispone de una base de licitud prevista en el artículo 6. 1 del RGPD. Pero ello no le excluye de la obligación adicional de disponer de una excepción prevista en el artículo 9 del RGPD cuando escoge un medio de control de horario que trate datos biométricos.

Al respecto, el Ayuntamiento aporta el Informe PRODAT que dice haber sido elaborado por el Delegado de Protección de Datos del Ayuntamiento de 24/11/20, lo que no se acredita, dado que aparece sin pie de firma, en el que se indica que "*el fichaje mediante reconocimiento facial supone un tratamiento de datos biométricos, que no tiene la consideración de categoría especial de datos al tratarse de un tratamiento técnico de verificación/autenticación biométrica (uno-a-uno), que debemos entender proporcional, en atención a las medidas higiénicas que se deben aplicar por la situación sanitaria que estamos viviendo por la pandemia COVID19".*

Mantiene el Ayuntamiento que dicho criterio es el seguido por esta Agencia en el Dictamen del Gabinete Jurídico de Agencia nº 36/2020, y la anterior "Guía sobre la Protección de Datos en las Relaciones Laborales" de mayo de 2021. No obstante, debe aclararse que esta interpretación ha sido superada y sustituida por el nuevo criterio fijado en las Directrices 05/2022 del Comité Europeo de Protección de Datos (CEPD), máxima autoridad europea en la materia, sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público de 26 de abril de 2023.

Las nuevas Directrices 05/2022 determinan, en su apartado 12, que el concepto de dato biométrico abarca tanto la "autenticación" como la "identificación", y si bien son conceptos distintos, en ambos procedimientos se tratan datos dirigidos a identificar a una persona física, por lo que ambos se incluyen en el concepto de "tratamientos de datos", y más específicamente, son tratamientos de datos personales de categorías especiales.

Siendo indubitado el hecho de que los datos biométricos son de categoría especial, no constan evidencias de que concurra una de las excepciones previstas del artículo 9.2

del RGPD que permita tratar datos biométricos como medio de control de la obligación legal de vigilar y controlar la jornada laboral de los empleados municipales.

Descartada la posibilidad de acudir en este caso a la excepción del artículo 9.2.g) (*tratamiento necesario para la satisfacción de un interés público*), de acuerdo con los criterios ya puestos de manifiesto con anterioridad por esta Agencia, a los que hace referencia el encargado del tratamiento, debe descartarse asimismo la concurrencia de la excepción del artículo 9.2.b) del RGPD, cuya aplicación se propone en el Protocolo de Implantación aportado como Documento 8 del escrito presentado por el encargado del tratamiento escrito.

La excepción del artículo 9.2. b) del RGPD se refiere a: "*cuando el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable de tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros.*

Tal y como esta Agencia ya ha manifestado en la Guía sobre tratamientos de control de presencia mediante sistemas biométricos, en el caso del estado español, esta referencia debe entenderse referida a que exista una reserva de ley, a los efectos previstos en el artículo 53 de la Constitución. De acuerdo a la doctrina del Tribunal Constitucional, en sentencias como la STC 76/2019, de 22 de mayo, o la STC 292/2000, de 30 de noviembre, la reserva de ley implicará que es necesario que exista una norma con rango de ley que habilite expresamente a la limitación del derecho fundamental de que se trate.

Aplicando esta doctrina a los supuestos de limitación del derecho fundamental a la protección de datos personales, y al supuesto presente, la aplicación de la excepción del artículo 9.2.b) del RGPD para poder tratar datos biométricos de los empleados para identificar-autenticar la identidad de una persona con la finalidad de controlar el cumplimiento de su jornada laboral, precisaría que exista una norma con rango de ley que habilite expresamente a que dicho control se realice mediante métodos que impliquen el tratamiento de datos biométricos.

En este orden de cosas, la Guía citada concluye que: "*en la actual normativa legal española no se contiene autorización suficientemente específica alguna para considerar habilitado el tratamiento de datos biométricos con la finalidad de un control horario de la jornada de trabajo, ni para el personal laboral, puesto que los artículos 20.3 y 34.9 del Texto Refundido del Estatuto de los Trabajadores (ET), no contienen dicha autorización, ni para el personal sometido a una relación jurídica administrativa, al no constituirse en necesaria habilitación la previsión relacionada con el cumplimiento de jornada y horario a la que alude el artículo 54.2 del Texto Refundido por el que se aprueba el Estatuto Básico del Empleado Público (TREBEP)".*

En este supuesto, tratándose de empleados municipales, cabe señalar que la previsión del artículo 21.1.h) de la Ley de Bases de Régimen Local 7/85, de 2 de abril, a la que hace referencia el Protocolo del encargado del tratamiento ni siquiera prevé expresamente la obligación de controlar la jornada y horario, puesto que se limita a atribuir la jefatura superior del personal municipal al Alcalde.

No habiéndose presentado alegaciones al acuerdo de inicio, ni habiéndose acreditado, por tanto, la concurrencia de ninguna de las excepciones previstas en el artículo 9.2 del RGPD que permita levantar la prohibición general de tratamiento de datos biométricos,

se confirma que al implantar el sistema de fichaje biométrico el Ayuntamiento ha incurrido, asimismo, una infracción administrativa del artículo 9 del RGPD.

VI. Tipificación y calificación de la infracción del artículo 9 del RGPD

Tal y como se ha expuesto en el Fundamento de Derecho V, de conformidad con las evidencias de las que se dispone en el presente momento, se confirma que los hechos expuestos vulneran lo establecido en el artículo 9 del RGPD, lo que podría suponer la comisión de una infracción administrativa tipificada en el artículo 83.5 del RGPD, que dispone lo siguiente:

> *"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por* la de mayor cuantía:
> "*a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9."*

A los efectos de prescripción, la LOPDGDD establece en su artículo 72.e):

> "*En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*
> "*e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 9 de esta ley orgánica*."

VII. Sobre la obligación de participación del DPD prevista en el artículo 38 del RGPD.

Otra de las grandes novedades que convierten al RGPD en un cambio de paradigma en materia de protección de datos es su configuración como un marco modernizado y basado en la rendición de cuentas para la protección de los datos personales en Europa, donde los delegados de protección de datos (DPD) son el elemento central, por facilitar al responsable y encargado del tratamiento el cumplimiento de las disposiciones del RGPD.

En torno a esta idea, los artículos 37 a 39 del RGPD, regulan los supuestos en que su designación es obligatoria, la posibilidad de designarlos voluntariamente, obligaciones como la de publicar sus datos de contacto y comunicarlos a la autoridad de control, así como su posición, y funciones dentro de la organización para la que es designado.

En concreto, y por lo que respecta al presente expediente, cabe hacer referencia a lo que establece el artículo 38 del RGPD, sobre la "Posición del delegado de protección de datos", que dispone lo siguiente:

> *1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.*

2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.

5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses".

En esta línea, las Directrices W243 sobre los Delegados de Protección de Datos del Grupo de Trabajo del artículo 29, aprobadas el 13 de diciembre de 2016, y revisadas el 5 de abril de 2017, remarcan la importancia de la obligación que tiene el responsable de hacer efectiva esta participación, consultando al DPD de su organización antes de adoptar decisiones que afecten a la protección de datos de forma previa y adecuada a cada tratamiento de datos personales que pretenda realizar.

"3.1. Participación del DPD en todas las cuestiones relativas a la protección de datos personales El artículo 38 del RGPD establece que el responsable y el encargado del tratamiento garantizarán que el DPD «participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales».

Es fundamental que el DPD, o su equipo, participen desde la etapa más temprana posible en todas las cuestiones relativas a la protección de los datos. En cuanto a las evaluaciones de impacto relativas a la protección de datos, el RGPD dispone expresamente la implicación temprana del DPD y especifica que el responsable del tratamiento recabará el asesoramiento del DPD al realizar dicha evaluación de impacto .Garantizar que se informa y consulta al DPD desde el principio facilitará el cumplimiento del RGPD, fomentará un enfoque de privacidad desde el diseño y, por lo tanto, debería ser un procedimiento estándar en la gobernanza de la organización. Asimismo, es importante que el DPD sea considerado como un interlocutor dentro de la organización y que forme parte de los correspondientes grupos de trabajo que

se ocupan de las actividades de tratamiento de datos dentro de la organización. En consecuencia, la organización debe garantizar, por ejemplo, que: Se invita al DPD a participar con regularidad en reuniones con los cuadros directivos altos y medios. Se recomienda que esté presente cuando se toman decisiones con implicaciones para la protección de datos. Toda la información pertinente debe transmitirse al DPD a su debido tiempo con el fin de que pueda prestar un asesoramiento adecuado. La opinión del DPD se tiene siempre debidamente en cuenta. En caso de desacuerdo, el Grupo de Trabajo recomienda, como buena práctica, documentar los motivos por los que no se sigue el consejo del DPD. Se consulta al DPD con prontitud una vez que se haya producido una violación de la seguridad de los datos o cualquier otro incidente. Cuando sea pertinente, el responsable o el encargado del tratamiento podría elaborar directrices o programas sobre la protección de datos que determinen cuándo debe consultarse al DPD".

Consta en el expediente que el DPD del Ayuntamiento – cuya designación es, en este caso, obligatoria de acuerdo con lo previsto en el artículo 37.1.a) del RGPD- no participó de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a protección de datos personales que suscitó el nuevo sistema de control de horario TARA implantado por el Ayuntamiento. Esto es, no consta la participación del DPD, ni la previa consulta del Ayuntamiento en ninguna de las fases de implantación de este tratamiento, ni previamente, ni durante, ni posteriormente al inicio de las ninguna de las 3 operaciones de tratamiento llevadas a cabo para controlar el horario de sus empleados municipales a partir del 2-11-21.

Preguntado al respecto por esta cuestión por el inspector en las actuaciones de investigación, el Ayuntamiento reconoce claramente que: "*No se solicitó informe del Delegado de Protección de Datos previamente al inicio de los citados tratamientos, existiendo un informe de fecha de 24 de noviembre de 2020 referente a idoneidad en relación a la posibilidad de implantación del fichaje laboral mediante reconocimiento facial en relación a las medidas higiénicas que se deben aplicar por la situación sanitaria por pandemia COVID19 cuando se trata de verificación/autenticación biométrica (uno-a-uno)*"

El citado Informe PRODAT de 24/11/2020 aportado por el Ayuntamiento, no contiene pie de firma ni se identifica a la persona u órgano emisor. Y ciñe su objeto de análisis a lo siguiente: "*Habiéndose realizado la consulta por parte del M.I. AYUNTAMIENTO DE TELDE en relación a la idoneidad de la implantación del fichaje laboral mediante el reconocimiento facial, se debe analizar si la implantación del sistema de reconocimiento facial es conforme a la normativa estatal vigente de protección de datos de carácter personal".*

Mediante la aportación de este informe, en el que no puede identificarse al órgano o persona emisor, no puede entenderse acreditado que dicho Informe fuera emitido por el DPD del Ayuntamiento, careciendo los documentos sin firma de validez jurídica.

Pero incluso en el caso de que el citado informe hubiera sido emitido por el DPD del Ayuntamiento, lo cierto es que dicho informe, por sí solo, no acreditaría tampoco que

la participación del DPD fuera “adecuada y previa al tratamiento” que finalmente fue implantado por el Ayuntamiento.

Ello es así, toda vez que dicho Informe PRODAT: (i) no analizó en su conjunto, todas las operaciones de tratamiento que finalmente se llevaron a cabo (que se ampliaron más allá del reconocimiento facial), (ii) ni entró a valorar todas las cuestiones de protección de datos que planteaba dicho tratamiento, atinentes al cumplimiento de todos los principios y requisitos exigidos por el RGPD para poder poner en marcha el nuevo sistema TARA de control de horario establecido en las citadas normas municipales (limitándose a analizar la cuestión que le fue consultada en el año 2020, sobre la idoneidad del reconocimiento facial). Ya que todas estas se consideran como “cuestiones sobre protección de datos personales” en las que es obligatoria su participación.

En consecuencia, de conformidad con las evidencias de las que se dispone en este acuerdo de iniciación del procedimiento sancionador, y no habiéndose formulado alegaciones al respecto ni aportado ninguna prueba que acredite la participación del DPD durante la fase de instrucción del presente procedimiento, se considera que los hechos conocidos son constitutivos de una infracción del artículo 38.1 del RGPD, que atribuye al responsable del tratamiento el deber de garantizar que el DPD participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

VIII. Tipificación y calificación de la infracción del artículo 38 del RGPD.

La vulneración del artículo 38 del RGPD se encuentra tipificada en el artículo 83.4.a) del citado RGPD en los siguientes términos:

> *“4. 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.”*

Por su parte, la LOPDGDD en su artículo 73, a efectos de prescripción, califica de *“Infracciones consideradas graves:*

> *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:*
> *w) No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.”*

IX. Propuesta de sanción

El artículo 83 "*Condiciones generales para la imposición de multas administrativas*" del RGPD en su apartado 7 establece:

> "*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."*

Asimismo, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone que:

> *"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:*
>
> *a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.*
> *b) Los órganos jurisdiccionales.*
> *c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.*
> *d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.*
> *e) Las autoridades administrativas independientes.*
> *f) El Banco de España.*
> *g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.*
> *h) Las fundaciones del sector público.*
> *i) Las Universidades Públicas.*
> *j) Los consorcios.*
> *k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.*
> *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 declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016".*
>
> *La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.*
> *3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.*

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.
4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.
5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo."

Perteneciendo el responsable del tratamiento a la administración local, de confirmarse la comisión de las citadas infracciones, correspondería dictar resolución declarando la infracción del artículo 35 del RGPD y del artículo 9 del RGPD por parte del Ayuntamiento de Telde.

X. Adopción de medidas correctoras

Confirmándose la comisión de las 3 infracciones imputadas en el presente procedimiento, procede, así mismo, imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "*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…".*

En este sentido, tales medidas deberán consistir en realizar y acreditar a esta Agencia en el **plazo de 7 meses** el cumplimiento de las siguientes medidas correctivas en atención al cumplimiento de los artículos 9 y 35 del RGPD:

- El Ayuntamiento deberá realizar y superar una EIPD, con la participación adecuada del DPD, que contenga un previo análisis de riesgos, y la evaluación del triple juicio de idoneidad, necesidad y proporcionalidad de cada una de las operaciones de tratamiento (sistemas de fichaje de la jornada laboral) que pretenda implantar, determine si concurre alguna de las excepciones del artículo 9.2.del RGPD, así como las medidas de protección adecuadas, y el resto de obligaciones requeridas por la normativa de protección de datos personales.
  En caso de que alguna de las operaciones de tratamiento en que se concretan los sistemas de fichaje implantados por el Ayuntamiento no supere el triple juicio señalado, y/o no concurra la excepción que permite tratar datos biométricos, o no sea posible cumplir con alguna de las obligaciones previstas en la normativa de protección de datos, el Ayuntamiento no podrá llevar a cabo la operación/es de tratamiento de que se trate, debiendo acreditar tal circunstancia ante esta Agencia.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una

infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

XI.
Elevación de medida provisional a definitiva. Prohibición de tratamiento.

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;"*

Respecto a la limitación temporal o definitiva del tratamiento, cabe referenciar el artículo 69 de la LPACAP, que determina:

> **"***1. Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de Protección de Datos podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos y, en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado.*
> *2. En los casos en que la Agencia Española de Protección de Datos considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos personales podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización."*

El artículo 56 de la LPACAP, señala en su apartado quinto que:

> *"5. Las medidas provisionales podrán ser alzadas o modificadas durante la tramitación del procedimiento, de oficio o a instancia de parte, en virtud de circunstancias sobrevenidas o que no pudieron ser tenidas en cuenta en el momento de su adopción. En todo caso, se extinguirán cuando surta efectos la resolución administrativa que ponga fin al procedimiento correspondiente*".

En el presente procedimiento, el Acuerdo de Inicio de procedimiento sancionador acordó lo siguiente:

> *"ORDENAR como medida provisional al* ***AYUNTAMIENTO DE TELDE****, con NIF* ***P3502600D****, de acuerdo con lo dispuesto en el artículo 69 de la LOPDGDD y artículo 56 de la LPACAP, la suspensión temporal de todo tratamiento de datos personales correspondiente a los sistemas de fichaje biométrico-y en especial de*

los referidos al sistema de reconocimiento facial- y fichaje a través de APP en el móvil con geolocalización de sus empleados como método de control de cumplimiento de la jornada laboral de sus empleados.

La medida provisional deberá llevarse a cabo en el plazo de diez días hábiles, contados desde la notificación de este acuerdo de apertura del procedimiento, y permanecerá hasta su resolución final, en que deberá ser confirmada, modificada o levantada, sin perjuicio de lo dispuesto en el art. 56.5 de la LPACAP, pudiendo acordarse en la resolución final la limitación definitiva o prohibición de dichas operaciones de tratamiento de acuerdo con lo previsto en los artículos 58 del RGPD y 69 de la LOPDGDD. A tal fin, deberá justificar ante esta Agencia Española de Protección de Datos la atención del presente requerimiento".

No obstante, a fecha de hoy el Ayuntamiento del Telde no ha presentado alegaciones al acuerdo de inicio ni comunicado a esta Agencia que haya cumplido con la medida de suspensión provisional de las operaciones de tratamiento de datos biométricos y de localización empleados para el fichaje de la jornada laboral de sus empleados, por lo que se desconoce si este sistema ha sido suspendido provisionalmente, tal y como se ordenaba en el acuerdo de inicio del procedimiento sancionador, o lo han suspendido definitivamente.

Se estima que persisten en la actualidad de forma indubitada los mismos riesgos que motivaron la suspensión o limitación provisional del tratamiento en el acuerdo de inicio, ya que la continuación de las operaciones de tratamiento de datos biométricos y de localización de los empleados derivada de los sistemas de fichaje de jornada laboral implementados por el Ayuntamiento podría comportar un menoscabo muy grave e irreparable para los derechos y libertades de los usuarios que accedan al estadio utilizando el sistema biométrico implantado.

Dadas las circunstancias, se entiende que la prohibición del tratamiento, como medida correctiva de las otorgadas en el artículo 58.2.f) del RGPD a la Agencia Española de Protección de Datos, es la única medida susceptible de ser adoptada para salvaguardar el Derecho Fundamental a la Protección de Datos, resultando ser, además, la menos lesiva, onerosa, proporcional y efectiva, así como la más proporcional y efectiva para el denunciado.

Desde estas premisas y a fin de garantizar los derechos y libertades de los afectados, se estima procedente confirmar la suspensión provisional ordenada en el acuerdo de inicio, y prohibir, como medida correctiva, el tratamiento de los datos personales a través de las operaciones de tratamiento que el Ayuntamiento califica como "sistema de fichaje biométrico" (huella/reconocimiento facial) y "sistema de fichaje a través de APP en el dispositivo móvil con geolocalización (sea en el dispositivo personal del empleado o en uno corporativo), procediendo a la cesación de ambas operaciones de tratamiento.

Esta medida no impediría al denunciado seguir controlando la jornada laboral de sus empleados de forma correcta y legal con los otros sistemas que ya está utilizando, dado que dispone de una tercera operación de tratamiento denominada "sistema de fichaje mediante internet, que permite la conexión vía web", y le es posible arbitrar con cierta facilidad otros métodos menos intrusivos de control de jornada (hojas de firmas, tarjetas magnéticas…etc) que ya fueron utilizados en el pasado, por lo que la suspensión de los sistemas de fichaje biométrico y por geolocalización no le supone un coste o esfuerzo

desproporcionado ni le impide continuar cumpliendo con su obligación legal de vigilar y controlar el cumplimiento de la jornada laboral de sus empleados.

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: DECLARAR que AYUNTAMIENTO DE TELDE, con NIF P3502600D, ha infringido lo dispuesto en el Artículo 38 del RGPD, Artículo 9 del RGPD y Artículo 35 del RGPD, habiendo cometido 3 infracciones tipificadas en el Artículo 83.4.a) del RGPD y Artículo 83.5.a) del RGPD.

SEGUNDO: Confirmar la medida provisional impuesta en el acuerdo de inicio del presente expediente sancionador, y prohibir al **AYUNTAMIENTO DE TELDE**, como medida correctiva prevista en el artículo 58.2.f) del RGPD, todo tratamiento de datos personales correspondiente a los sistemas de fichaje biométrico-y en especial de los referidos al sistema de reconocimiento facial- y fichaje a través de APP en el móvil con geolocalización de sus empleados como método de control de cumplimiento de la jornada laboral de sus empleados. A estos efectos, deberá acreditar en el plazo de diez días hábiles desde que la presente resolución sea firme y ejecutiva ante esta Agencia Española de Protección de Datos que ha procedido a la cesación de estas dos operaciones de tratamiento.

TERCERO: ORDENAR a ***AYUNTAMIENTO DE TELDE***, con NIF ***P3502600D***, que en virtud del artículo 58.2.d) del RGPD, en el plazo de 7 meses desde que la presente resolución sea firme y ejecutiva, acredite haber procedido al cumplimiento de las siguientes medidas correctivas en atención al cumplimiento de los artículos 9 y 35 del RGPD:

- El Ayuntamiento deberá realizar y superar una EIPD, con la participación adecuada del DPD, que contenga un previo análisis de riesgos, y la evaluación del triple juicio de idoneidad, necesidad y proporcionalidad de cada una de las operaciones de tratamiento (sistemas de fichaje de la jornada laboral) que pretenda implantar, determine si concurre alguna de las excepciones del artículo 9.2.del RGPD, así como las medidas de protección adecuadas, y el resto de obligaciones requeridas por la normativa de protección de datos personales.

- En caso de que alguna de las operaciones de tratamiento en que se concretan los sistemas de fichaje implantados por el Ayuntamiento no supere el triple juicio señalado, y/o no concurra la excepción que permite tratar datos biométricos, o no sea posible cumplir con alguna de las obligaciones previstas en la normativa de protección de datos, el Ayuntamiento no podrá llevar a cabo la operación/es de tratamiento de que se trate, debiendo acreditar tal circunstancia ante esta Agencia.

CUARTO: NOTIFICAR la presente resolución a ***AYUNTAMIENTO DE TELDE***.

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

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

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

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

938-16012024

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