- **Expediente N.º: EXP202302938**

Procedimiento Sancionador PS/00545/2023

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, el reclamante) con fecha 15 de mayo de 2023 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra el ***AYUNTAMIENTO DE FUENTEPELAYO*** con NIF ***P4010000J*** (en adelante, el Ayuntamiento). Los motivos en que basa la reclamación son los siguientes:

El reclamante trabaja (…) de la residencia de ancianos de San Miguel, titularidad del Ayuntamiento de Fuentepelayo (Segovia), y expone lo siguiente:

- Que entre el 01/07/2021 y el 15/12/2022, la dirección de la residencia decidió instalar unilateralmente un reloj de fichajes como medio de registro de la jornada de los trabajadores, siendo obligatorio registrar la entrada y salida fichando mediante huella dactilar, sin comunicación ni información previa a los trabajadores ni a sus representantes, y sin aparente estudio de impacto.

- Que según van llegando los trabajadores de la empresa, se van registrando sus huellas dactilares, conociendo que no fueron tomadas las huellas de todos los trabajadores.

- Paralelamente a este sistema de fichaje, manifiesta el dicente que los trabajadores rellenaban una "hoja de control horario", que se utilizaba solo para comprobar los días festivos o turnos de nocturnidad.

- El reclamante solicitó información relativa a la protección de datos de los fichajes realizados por huella dactilar y extracto de los fichajes realizados a partir de 01/01/2022 a la dirección de la Residencia, al Jefe de RRHH y al Alcalde. Expone que le denegaron la información en una primera ocasión, argumentando que se trataba de un documento interno de control. Al insistir, se retiró el reloj de fichaje el 15-12-22, sin previa comunicación del motivo a los trabajadores ni a este mismo. Posteriormente, volvió a solicitar nuevamente dicha información y la dirección le denegó su solicitud argumentando que los fichajes dactilares solo se utilizaron para verificar las hojas de firmas y que han sido destruidos, no existiendo la obligación de conservarlos porque el sistema de control oficial eran las hojas de control horario y no la huella dactilar (22/12/2022).

Junto al escrito de reclamación aporta:

- Fotografía del reloj de fichaje por huella dactilar realizada con carácter previo a su retirada el 15/12/2022, y fotografías de 3 carteles informativos firmados por

el Director de la Residencia: (i) de fecha 28/05/2021, 2 carteles, uno indicando "*Máquina de fichar: prohibido desenchufar bajo ningún concepto*"; y el otro con las "Normas para fichar" por huella dactilar, en el que se indica claramente: "*Al entrar a trabajar: todos los trabajadores ficharán uniformados. Al salir: todos los trabajadores ficharán uniformados (…)*"; (ii) y otro de 30/06/2021 que indicaba literalmente: "*A partir de julio se tendrá que fichar mediante huella dactilar y se seguirán usando las hojas de firmas. Dichas hojas servirán a cada trabajador para justificar y comprobar las horas realizadas mensualmente cuando se vayan a comunicar los datos al Ayuntamiento (nocturnidad, festivos, sábados y domingos). En caso de conflicto, la información contenida en los fichajes tendrá prevalencia sobre la anotada en la hoja de firmas*".

- También acompaña copia de los correos electrónicos intercambiados con la Residencia en el correo **residencia@fuentepelayo.es** para solicitar copia de sus fichajes, los dos últimos con copia a la alcaldía: (i) la solicitud remitida el 12/12/2022 y la contestación del mismo día indicando que debían solicitarse los fichajes mediante escrito al Ayuntamiento por ser una herramienta de gestión interna; (ii) la reiteración de la petición al mismo correo formulada el 21/12/22, que fue contestada el mismo día indicando que se había retirado el reloj, (iii) y el último del mismo día en el que el reclamante insiste en solicitar estos datos y se le responde los fichajes se usaron para verificar la hoja de firmas, y que fueron destruidos posteriormente porque no existe obligación de guardarlos.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), el 6/3/23 se dio traslado de dicha reclamación al Ayuntamiento reclamado, por ser dicha residencia de ancianos de titularidad municipal, para que contestasen al requerimiento de determinada información necesaria para cumplir con la normativa de tratamiento de datos biométricos, al objeto de que informase a esta Agencia en el plazo de un mes sobre la información solicitada.

El traslado, que se practicó 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), fue recogido en fecha 10/03/2023, como consta en el acuse de recibo que obra en el expediente.

TERCERO: Con fecha 31/03/2023, se recibe en esta Agencia escrito de respuesta del Ayuntamiento de Fuentepelayo, indicando, en síntesis, lo siguiente:

- Se identifica al Ayuntamiento como responsable del tratamiento de los datos personales de la residencia San Miguel, manifestando haber iniciado el tratamiento de los datos biométricos de los trabajadores de la misma (huellas dactilares) con la siguiente finalidad: "*como medida alternativa de control de presencia y registro de horarios de entradas y salidas de los trabajadores, con la finalidad de corregir impuntualidades que pudieran perturbar el correcto funcionamiento del servicio*".
- Se hace constar que: "*así como medio de verificación del cumplimiento de la normativa en materia de registro de jornada, se coloca este sistema alternativo, en pruebas, no existiendo huellas almacenadas, ni tampoco el registro de*

horarios, ni plantillas biométricas de datos, al ser suprimido el sistema, tras advertir diversos errores en su funcionamiento".

- Como base de licitud se alega lo previsto en el artículo 6.1.b) del RGPD (por ser necesario para la ejecución del contrato), y del artículo 6.1.e) del RGPD (en interés público).
- Como excepción a la prohibición general de tratamiento de datos personales biométricos alega la concurrencia de la causa del artículo 9.2.b), manteniendo que el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable.
- Al requerimiento de garantías adoptadas, no aporta ninguna, manteniendo únicamente que se halla adherido a un Plan de Asistencia para la protección de datos, e insistiendo en que no se almacenan las huellas, por lo que no cabe la reutilización de los datos, ni su supresión o destrucción. No obstante, se dice asimismo que los datos no se podían descifrar ni utilizar debido a los problemas técnicos advertidos.
- Respecto a la información previa a proporcionar a los trabajadores sobre el tratamiento de sus datos biométricos manifiesta que "*Los destinatarios del sistema eran el personal laboral de la Residencia de Ancianos. El sistema en pruebas, fue implantado en el local mediante anuncios y cartelería informativa, siendo el propio Director de la Residencia el encargado de informar individualmente a los trabajadores sobre el tratamiento de los datos que pudieran obtenerse*".
- Se reconoce que "*no se pudo realizar Evaluación de Impacto, como consecuencia de los fallos técnicos que propiciaba la instalación de este posible mecanismo, y, por otro lado, porque el mismo no pretendía sustituir al fichaje de registros manual que se encuentra en vigor a día de hoy, y que no almacena ningún tipo de huella*".
- Se manifiesta que el sistema fue retirado debido a problemas técnicos, manteniendo que: "*Esta Entidad Local entiende que se ha producido un malentendido en cuanto al funcionamiento y registro de la máquina de fichajes instalada, puesto que no cumplía con una función de almacenamiento de huella ni cualquier otro dato biométrico que pudiera requerir de una protección especial, consecuencia de su incorrecta instalación y por lo tanto funcionamiento*".
- Por último, respecto a las medidas adoptadas para garantía de los derechos de los interesados, informan de las que se adoptarían a futuro en caso de implantar el sistema de nuevo, pero no de las ya adoptadas.

CUARTO: Con fecha de 21 de abril de 2023 de conformidad con el artículo 65 de la LOPDGDD, se inadmitió a trámite la reclamación presentada por la parte reclamante, por considerar, principalmente, que el Ayuntamiento reclamado había procedido a retirar el sistema, por lo que se había atendido la reclamación presentada.

QUINTO: Con fecha de 15 de mayo de 2023 se presenta recurso de reposición por el reclamante frente a la resolución de inadmisión a trámite antes citada, y tras requerirse subsanación al mismo por falta de firma, se recibe el recurso en legal forma en esta Agencia el 2 de noviembre de 2023, y se da audiencia al Ayuntamiento reclamado con fecha de 3 de noviembre, sin que este diera respuesta al mismo.

SEXTO: Con fecha de 30 de noviembre de 2023, se dicta Resolución por la Directora General de esta Agencia estimando el recurso de reposición interpuesto, que se notifica al reclamante, a la vista de que de la documentación aportada en el recurso y la revisión de los antecedentes obrantes en el expediente se desprenden indicios suficientes de que el sistema de huella dactilar instalado por el Ayuntamiento no cumplía con la normativa de protección de datos aplicable a datos de categoría especial, cuyo tratamiento es de alto riesgo, como los biométricos. Como consecuencia de ello, se acuerda admitir a trámite la reclamación presentada el 15 de mayo de 2023, notificándose al reclamante.

SÉPTIMO: Con fecha 18 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 9 del RGPD, Artículo 35 del RGPD y Artículo 13 del RGPD, tipificada en el Artículo 83.4.a) del RGPD, Artículo 83.5.a) del RGPD y Artículo 83.5.b) del RGPD.

OCTAVO: Notificado el citado acuerdo de inicio 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) 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: El Ayuntamiento de Fuentepelayo reconoce en su escrito de 31 de marzo de 2023 que entre el 1 de julio de 2021 y el 15 de diciembre de 2022 implantó con la finalidad de registro de jornada del personal laboral de la residencia de ancianos de San Miguel, que es titularidad del Ayuntamiento, un sistema obligatorio de fichaje a través de huella dactilar, con la siguiente finalidad: "*como medida alternativa de control de presencia y registro de horarios de entradas y salidas de los trabajadores, con la finalidad de corregir impuntualidades que pudieran perturbar el correcto funcionamiento del servicio*". Reconoce y manifiesta que las huellas de los empleados fueron recogidas y almacenadas, y que el sistema de fichaje mediante huella dactilar fue utilizado por los empleados de la misma como sistema obligatorio de fichaje de

jornada, según consta en los carteles informativos que fueron colocados por la dirección de la residencia, aportados por la parte reclamante, que es empleado de la residencia. Por último, se manifiesta que fue suprimido el sistema el 15 de diciembre de 2022, *"tras advertir diversos errores en su funcionamiento"*, si bien no detalla de qué fallos técnicos se trata ni presenta acreditación de los mismos.

SEGUNDO: El Ayuntamiento reconoce que no ha realizado una EIPD previa ni posterior al inicio del tratamiento de datos biométricos (huella dactilar) de los empleados de la residencia.

TERCERO: No se ha acreditado por el Ayuntamiento que concurra ninguna de las excepciones previstas en el artículo 9.2 del RGPD que permita levantar la prohibición general de tratamiento de datos biométricos para la finalidad de registro y control de jornada del personal laboral de la residencia.

CUARTO: Respecto a la información previa a proporcionar a los trabajadores sobre el tratamiento de sus datos biométricos a la que se refiere el artículo 13 del RGPD, el Ayuntamiento manifiesta que "*Los destinatarios del sistema eran el personal laboral de la Residencia de Ancianos. El sistema en pruebas, fue implantado en el local mediante anuncios y cartelería informativa, siendo el propio Director de la Residencia el encargado de informar individualmente a los trabajadores sobre el tratamiento de los datos que pudieran obtenerse*".

No habiéndose aportado acreditación alguna que acredite que el Director proporcionó dicha información individualmente a los trabajadores, la única prueba que consta aportada al respecto son las fotografías de los 3 carteles informativos que fueron aportados por el reclamante, como reconoce la parte reclamada en la respuesta que dio al traslado de la reclamación, que están datados de 25 de mayo y 31 de junio de 2021, esto es, pocos días antes de la instalación del sistema biométrico de control, con el siguiente contenido:

(i) Cartel fecha 28/05/2021, indicando "*Máquina de fichar: prohibido desenchufar bajo ningún concepto*".

(ii) Cartel de 28/05/2021 con las "Normas para fichar" por huella dactilar, en el que se indica claramente: "*Al entrar a trabajar: todos los trabajadores ficharán uniformados. Al salir: todos los trabajadores ficharán uniformados (…)*".

(iii) El más relevante, de 30/06/2021 que indicaba literalmente: "*A partir de julio se tendrá que fichar mediante huella dactilar y se seguirán usando las hojas de firmas. Dichas hojas servirán a cada trabajador para justificar y comprobar las horas realizadas mensualmente cuando se vayan a comunicar los datos al Ayuntamiento (nocturnidad, festivos, sábados y domingos). En caso de conflicto, la información contenida en los fichajes tendrá prevalencia sobre la anotada en la hoja de firmas*".

QUINTO: De acuerdo con los correos electrónicos aportados por el reclamante, consta acreditado que éste solicitó información relativa a la protección de datos de los fichajes realizados por huella dactilar y extracto de los fichajes realizados a partir de

01/01/2022 a la dirección de la Residencia, al Jefe de RRHH y al Alcalde. En concreto, se acompaña copia de los correos electrónicos intercambiados con la Residencia en el correo **residencia@fuentepelayo.es** para solicitar copia de sus fichajes, los dos últimos con copia a la alcaldía: (i) la solicitud remitida el 12/12/2022 y la contestación del mismo día indicando que debían solicitarse los fichajes mediante escrito al Ayuntamiento por ser una herramienta de gestión interna; (ii) la reiteración de la petición al mismo correo formulada el 21/12/22, que fue contestada el mismo día indicando que se había retirado el reloj, (iii) y el último del mismo día en el que el reclamante insiste en solicitar estos datos y se le responde los fichajes se usaron para verificar la hoja de firmas, y que fueron destruidos posteriormente porque no existe obligación de guardarlos.

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
Datos biométricos como datos personales de categoría especial

2.1. Definición y características de los datos biométricos.

Los sistemas de procesamiento de datos biométricos se basan en recoger y procesar datos personales relativos a las características físicas, fisiológicas o conductuales de las personas físicas, entre las que cabe incluir las características neuronales de estas, mediante dispositivos o sensores, creando plantillas biométricas (también denominadas firmas o patrones) que posibilitan la identificación, seguimiento o perfilado de dichas personas.

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*".

Todo sistema biométrico de control de registro de jornada laboral, para poder ser usado, ha de registrar antes la identidad del usuario en el sistema por medio de la captura de

una serie de parámetros biométricos (en este caso, la huella de los trabajadores de la residencia). Lo que se trata de conseguir es realizar un procesamiento sobre esos parámetros para identificar a la persona cada vez que luego vuelva a entrar y salir por el punto de acceso.

La decisión de implantar un nuevo método de control de jornada laboral de los empleados que implique el tratamiento de datos biométricos, como los basados en la detección de huella dactilar, como es el caso presente (o reconocimiento facial en otros supuestos), no es una decisión baladí. Este tipo de tratamientos se basan en una tecnología puede ser realmente intrusiva y requiere de un debate ético y jurídico sosegado antes de decidir su implantación -incluso aunque estuviera en fase de pruebas-, toda vez que recoger la huella dactilar del personal puede tener efectos muy adversos en los valores fundamentales y la integridad humana de estos empleados que no se producen con otros métodos de control de asistencia. Véanse solo alguna de sus características especiales y piénsese en el impacto significativo que producen cuando se comprometen estos datos biométricos, en comparación a otros métodos (firma y cumplimentación de hojas, o fichaje mediante tarjetas magnéticas):

- Cada individuo tiene impresiones dactilares únicas que muestran características específicas que pueden medirse para decidir si una impresión dactilar corresponde con una muestra registrada. Por lo tanto, 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.

2.2. Las plantillas biométricas como datos personales de categoría especial y alto riesgo.

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, que define a los datos personales como:

> "1. 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 no cabe duda de que se están tratando datos biométricos de carácter personal, puesto que la finalidad del sistema implantado es determinar la identidad, directa o indirectamente, del empleado de la residencia que accede o sale 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 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".

Hay que tener en cuenta que la aprobación del RGPD ha supuesto un cambio de paradigma en materia de protección de datos personales que pretende garantizar aún más a los ciudadanos el control de sus datos personales, estableciendo unos estándares de protección elevados y adaptados al entorno digital en que vivimos. De acuerdo con el Principio de Responsabilidad Proactiva, inspirador 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. Así mismo, se deben cumplir determinadas obligaciones y respetar ciertos principios establecidos por la normativa.

Así pues, siempre que se traten datos de carácter personal, de cualquier tipo que sean, el responsable deberá cumplir con los principios y obligaciones previstos en la normativa de protección de datos para todo tipo de datos personales.

Pero cuando los datos personales a tratar sean biométricos (huellas, reconocimiento facial...etc), se debe considerar además que -a diferencia de lo que sucedía bajo el régimen anterior al RGPD- este tipo de datos 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*". Si bien el considerando 51 del RGPD incluye tanto procedimientos de identificación como de autenticación: *"pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de*

ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento".

En este sentido, hay que resaltar que la calificación como datos de categoría especial implica, necesariamente, la observancia de una especial cautela a la hora de determinar si es posible llevar a cabo un tratamiento de datos de esta naturaleza. Entre otras cosas, y además de existir una excepción que permita salvar la prohibición del artículo 9.1 del RGPD, de que exista una base de licitud del artículo 6 del RGPD y de que se cumplan los principios del RGPD, el sujeto que pretenda implantar sistemas de datos biométricos, en este caso, el Ayuntamiento debería haber analizado previamente la concurrencia de los preceptivos criterios de necesidad, idoneidad y proporcionalidad del tratamiento.

Esto es, quien pretenda instaurar un tratamiento de datos personales de esta naturaleza debe, antes que nada, asegurarse de que se supere lo que se ha denominado en la jurisprudencia como "el triple juicio de proporcionalidad", planteándose en especial si el tratamiento de datos biométricos es idóneo, proporcionalidad, y sobre todo, necesario. Si existen otros sistemas no biométricos que permitan conseguir la misma finalidad de identificar-verificar la identidad de las personas con eficacia, no será necesario iniciar tratamientos biométricos, y, por tanto, implantar este sistema se considerará contrario al RGPD. Este juicio debe ser el punto de partida de su análisis, pues sólo en caso de que estos métodos superen el citado triple juicio, se exigirá el cumplimiento de otros requisitos o garantías.

Juicio que el Ayuntamiento no ha realizado antes de iniciar el tratamiento el 1 de julio de 2021 (que es cuando debe hacerse), pero tampoco durante ni al final del tratamiento, pues dice haber retirado el sistema finalmente el 15-12-22 por motivos técnicos, sin plantearse si realmente lo que acontece es que existen otros métodos alternativos que permiten acreditar de forma unívoca la identidad de los trabajadores que entran y salen del centro de trabajo con la finalidad de controlar la jornada laboral, que no son tan intrusivos como los de detección de huella, y son igualmente idóneos para cumplir la función legal de control de jornada de trabajo.

Pero además de ser datos de categoría especial, el **tratamiento de datos biométricos se considera de alto riesgo** a tenor de lo previsto en el apartado 4 del artículo 35, que dispone que "…La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1…", dado que consta entre los tratamientos incluidos en la Lista de tipos de tratamiento de datos que requieren evaluación de impacto relativa a la protección de datos, hecho público por la AEPD en desarrollo de la previsión contemplada en el apartado cuarto del referido artículo 35.

No hay duda del carácter de alto riesgo de estos datos, habida cuenta de que los datos biométricos cumplen con los criterios correspondientes a los números 4, 5 y 10 de dicho documento (aquellos que impliquen el uso de categorías especiales de datos; el uso de datos biométricos y los que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas). Por tanto, el tratamiento de datos biométricos nunca podrá iniciarse de no haber elaborado y superado una EIPD válida y previa al tratamiento.

Cuando un tratamiento es de “alto riesgo”, como sucede con los métodos de control de jornada laboral basados en métodos de fichaje biométricos, es obligatorio realizar siempre una evaluación de impacto (EIPD), de acuerdo con lo previsto en el artículo 35.1 del RGPD, debiendo esta EIPD ser previa al inicio del tratamiento, pero realizarse a su vez de forma continua. Y no bastará con realizarla, sino que la misma deberá considerarse válida, porque cumpla con los requisitos previstos en el citado artículo, en especial, que contenga como mínimo la información del art. 35.7 del RGPD.

Consta acreditado que el Ayuntamiento no realizó una EIPD en este supuesto. De haber realizado esta EIPD de forma adecuada y antes de iniciar el tratamiento -como es legalmente preceptivo al ser de alto riesgo-, el Ayuntamiento hubiera podido valorar y determinar si este tratamiento cumplía los requisitos legales antes de iniciarlo, sin incurrir en las infracciones administrativas cuya responsabilidad dilucida este procedimiento.

2.3. El Ayuntamiento de Fuentepelayo como responsable de operaciones de tratamiento de datos biométricos del personal laboral de la Residencia.

El artículo 4.2 del RGPD define el “tratamiento de datos personales” como:

> *“cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto 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;”*

Las características biométricas se someten a un tratamiento técnico mediante el cual se reconoce a una persona a través de un proceso cronológico que se contiene en todos los tratamientos de datos biométricos: su captura o registro de datos con su siguiente almacenamiento o procesamiento y la fase de comparación o correspondencia, la conservación de los datos, así como su posterior supresión, limitación…etc.

Y si el tratamiento consiste en el registro diario de la jornada laboral, ello requiere realizar un conjunto variado de operaciones que requieren el tratamiento de datos personales biométricos, entre las que cabe incluir: la identificación del empleado, la recogida o captura de su huella (sea en bruto o a través de un vector), su registro, almacenamiento, la identificación-autenticación de este en el proceso de fichaje, el registro de tiempo y otros posibles datos, su procesamiento para determinar los excesos o faltas horarias, su conservación, supresión, limitación…etc).

Aunque el Ayuntamiento insiste en que el sistema biométrico ha sido retirado, lo cierto es que consta acreditado que ha habido un tratamiento previo de datos biométricos que incumplió con los requisitos previstos legalmente. Pues algunas de estas operaciones de tratamiento debieron realizarse necesariamente durante el periodo en que estuvo implantado el sistema de huella, independientemente de que fuera cierto que se produjesen problemas técnicos, o de que tras su retirada no se hayan archivado los datos (ni huellas ni registros de entrada y salida..etc), o de que al recoger la huella no se obtuviese un vector biométrico, dado que se reconoce y manifiesta que las huellas fueron recogidas y el sistema utilizado como sistema obligatorio de fichaje de jornada, según consta en los carteles informativos que fueron colocados por la dirección de la residencia.

En su virtud, pese a que el sistema se haya retirado, e incluso en el caso de ser cierto que se han suprimido los datos almacenados (lo que no se acredita), lo cierto es que entre el 1 de julio de 2021 y el 15 de diciembre de 2022 el Ayuntamiento reclamado fue responsable de las operaciones de tratamiento de datos biométricos que se llevaron a cabo para poner en funcionamiento el sistema (registro huellas, almacenamiento en sistema, identificación-autenticación de identidad que aparece al fichar en el reloj, procesamiento, utilización, etc).

El propio Ayuntamiento se declara responsable del tratamiento de datos personales de la Residencia en su escrito de 31 de marzo de 2023, por lo que es sin duda el responsable de la posible responsabilidad sancionadora que se derive del incumplimiento de las obligaciones previstas en materia de protección de datos a los efectos previstos en el artículo 4. 7 del RGPD, que 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".*

En definitiva, cuando el Ayuntamiento reclamado implantó un nuevo sistema de detección de huella dactilar para la identificación-verificación de la identidad de personas físicas debió ser consciente de que iba a pasar a ser responsable de fijar los fines y medios de varias operaciones de tratamiento de datos de categoría especial y de alto riesgo, y que ello requiere del cumplimiento de unos requisitos previos, sea para instalarlo en fase de pruebas, o no, puesto que al registrar las huellas y registrarse la jornada se están ya tratando datos biométricos, con independencia de que el sistema esté produciendo efectos jurídicos a los efectos de cumplimiento de jornada o no.

De las evidencias que obran hasta el momento en el expediente, tras la instrucción practicada, se deduce que el Ayuntamiento implantó este sistema cometiendo 3 infracciones administrativas en los términos que se exponen a continuación en los Fundamentos de Derecho III al V de esta Resolución..

III.

Sobre la necesidad de realizar una evaluación de impacto previa y adecuada al tratamiento.

Tal y como se ha expuesto anteriormente, antes de implantar un proyecto de tratamiento de datos basado en esta tecnología tan intrusiva, es preciso también auditar previamente su funcionamiento, no de forma aislada sino en el marco del tratamiento concreto en que se va a emplear (en este caso, registro diario de la jornada laboral a los empleados del Ayuntamiento).

La evaluación de impacto en la protección de datos personales, EIPD, aparece entonces como la herramienta exigida por el RGPD para garantizar que se cumple con esta vertiente del tratamiento, según lo establecido en el artículo 35 en su apartado- 1 del RGPD,

> *"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…"*

Como ya se ha indicado, el tratamiento de datos biométricos ha sido calificado de alto riesgo por la AEPD, en virtud de lo previsto en el artículo 35.4 del RGPD, por lo que debemos partir de la base de que el tratamiento de datos biométricos implantado por el Ayuntamiento debió estar precedido de una evaluación de impacto válida, que incluyese como mínimo los apartados previstos en el artículo 35.7 del RGPD. Ello implica que no basta con realizar una EIPD, sino que habrá que superarla para cumplir con el RGPD.

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, el Ayuntamiento reclamado reconoce que inició el tratamiento el 1 de julio de 2021 y lo mantuvo hasta el 15 de diciembre de 2022 con la finalidad de registro de jornada del personal laboral de la residencia pero que no realizó una EIPD, en base a la siguiente argumentación: "*no se pudo realizar Evaluación de Impacto, como consecuencia de los fallos técnicos que propiciaba la instalación de este posible mecanismo, y, por otro lado, porque el mismo no pretendía sustituir al fichaje de*

registros manual que se encuentra en vigor a día de hoy, y que no almacena ningún tipo de huella".

Como ya se ha anticipado, lo que determina la necesidad de realizar una EIPD no tiene que ver con los efectos jurídicos que vaya a producir el sistema biométrico de huella dactilar en el control de jornada laboral, por lo que es indiferente que este sistema fuera principal o complementario para cumplir con esta función, o que estuviera en fase de pruebas, lo que no ha sido acreditado por el Ayuntamiento.

Y también es indiferente el hecho de que el sistema instalado tuviera unos presuntos fallos técnicos y se retirase por este motivo. Fallos técnicos que no se detallan ni acreditan por el Ayuntamiento, que no aporta certificado ni informe técnico alguno que los justifique, ni concreta en qué fase del procedimiento técnico del sistema se producían, ni por tanto, a qué operaciones del tratamiento estaban presuntamente afectando (registro de huella, almacenamiento, procesamiento, verificación de la identidad…etc). Pero que, en cualquier caso, son del todo irrelevantes porque la obligación de elaborar una EIPD incumbe a todo responsable que se plantee realizar un tratamiento de alto riesgo, antes de realizarlo, para poder analizar previamente a su implantación si la finalidad que pretende cumplir con los métodos biométricos es realmente necesaria, proporcional e idónea, tras analizar todos los riesgos concurrentes y si la misma finalidad no puede lograrse utilizando otros métodos menos intrusivos.

Lo realmente relevante es que se ha acreditado que el sistema estuvo instalado y funcionando (bien o mal) durante casi año y medio, lo que implicó la recogida de los datos biométricos, que se debieron almacenar necesariamente durante dicho tiempo y utilizar para realizar la identificación en cada entrada y salida, aunque concurriesen defectos técnicos. Por tanto, hubo tratamiento de datos de alto riesgo por la entidad responsable, sin haberse realizado una previa EIPD, que era obligatoria según el artículo 35 del RGPD, por lo que el Ayuntamiento incurrió en una presunta infracción del citado precepto.

IV

Concurrencia de una excepción del artículo 9 del RGPD, y base legitimadora del artículo 6 del RGPD.

Otro de los requisitos adicionales de este tipo de tratamientos será por tanto que previamente a iniciar el tratamiento el responsable deberá también comprobar y acreditar que concurra una de las excepciones previstas en el artículo 9.2 del RGPD u otra legislación específica.

Hay que señalar que, estando prohibido su tratamiento 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.

Preguntados por la circunstancia del artículo 9.2 del RGPD que permitiese al Ayuntamiento tratar estos datos, éste manifiesta que se ampara en el apartado b), referido a que el tratamiento sería necesario para el cumplimiento de una obligación legal, que, si bien no se concreta, puede entenderse que se refiere a la obligación de controlar el cumplimiento de la jornada laboral por los empleados públicos y la correlativa del personal de someterse a tal control establecido por la administración. En concreto, a la obligación de controlar la jornada laboral del personal laboral de la residencia de titularidad municipal.

No concurriendo, por tanto, la excepción de tratamiento de datos biométricos del cumplimiento de una obligación legal prevista en el derecho español, ni habiéndose acreditado la concurrencia de ninguna otra excepción prevista en el artículo 9.2 del RGPD, se considera que el tratamiento biométrico realizado por el Ayuntamiento, ha incurrido, asimismo, en una infracción administrativa del artículo 9 del RGPD.

A mayor abundamiento, debe aclararse que no se cuestiona que el Ayuntamiento actúe con una base de licitud prevista en el artículo 6. 1.b), puesto que se trata de empleados laborales con los que debe tenerse una relación contractual, por lo que se puede considerar inicialmente que el tratamiento de sus datos personales "*es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales".* Por tanto, no cabe inicialmente imputar una infracción del artículo 6 del RGPD.

Ahora bien, la base de licitud del artículo 6 del RGPD puede legitimar al Ayuntamiento para tratar datos personales no biométricos, que permiten llevar un registro y control de presencia mediante otros métodos tradicionales (hojas firmadas, tarjetas…etc), pero en ningún caso legitima para iniciar un tratamiento biométrico, si no concurre una de las excepciones del artículo 9.2 del RGPD.

En el presente supuesto, cabe aclarar que no cabe admitir la excepción del artículo 9.2. b) del RGPD, que 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 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 considera que al implantar el sistema de fichaje biométrico el Ayuntamiento ha incurrido, asimismo, en una infracción administrativa del artículo 9 del RGPD.

V

Sobre los deberes de información del artículo 13 del RGPD

Por último, cabe recordar que una de las obligaciones del responsable de todo tratamiento de datos personales es cumplir con los deberes de información a los interesados que vienen previstos en los artículos 12 a 14 del RGPD.

De acuerdo con lo previsto en el artículo 12.1 de RGPD, se parte de un Principio de "*Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado*":

> "1. *El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios*"

Estos deberes de información se concretan en los artículos 13 y 14, siendo de aplicación al supuesto presente, los previstos en el artículo 13 del RGPD sobre "*Información que deberá facilitarse cuando los datos personales se obtengan del interesado":*

> *1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:*

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos;
f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.
4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información".

En el presente supuesto, respecto a la información previa a proporcionar a los trabajadores sobre el tratamiento de sus datos biométricos, el Ayuntamiento manifiesta que "*Los destinatarios del sistema eran el personal laboral de la Residencia de*

Ancianos. El sistema en pruebas, fue implantado en el local mediante anuncios y cartelería informativa, siendo el propio Director de la Residencia el encargado de informar individualmente a los trabajadores sobre el tratamiento de los datos que pudieran obtenerse".

No habiéndose aportado acreditación alguna sobre la información individual a los trabajadores por el Director, la única prueba que consta aportada al respecto son las fotografías de los 3 carteles informativos que fueron aportados por el reclamante, que están datados de 25 de mayo y 31 de junio de 2021, esto es, pocos días antes de la instalación del sistema biométrico de control, con el siguiente contenido:

(i) Cartel fecha 28/05/2021, indicando "*Máquina de fichar: prohibido desenchufar bajo ningún concepto*".

(ii) Cartel de 28/05/2021 con las "Normas para fichar" por huella dactilar, en el que se indica claramente: "*Al entrar a trabajar: todos los trabajadores ficharán uniformados. Al salir: todos los trabajadores ficharán uniformados (…)*".

(iii) El más relevante, de 30/06/2021 que indicaba literalmente: "*A partir de julio se tendrá que fichar mediante huella dactilar y se seguirán usando las hojas de firmas. Dichas hojas servirán a cada trabajador para justificar y comprobar las horas realizadas mensualmente cuando se vayan a comunicar los datos al Ayuntamiento (nocturnidad, festivos, sábados y domingos). En caso de conflicto, la información contenida en los fichajes tendrá prevalencia sobre la anotada en la hoja de firmas*".

De los carteles informativos colocados se deduce lo siguiente:

- Que a partir del 1-7-21 el fichaje biométrico tenía carácter obligatorio y principal, indicándose claramente que el mismo prevalecerá frente a posibles contradicciones con la hoja de firmas. Por tanto, el sistema no era complementario al de las hojas, como manifiesta el Ayuntamiento. O, al menos, ello fue lo que se informó formalmente a los empleados.

- No existe en los carteles referencia alguna a que el sistema estuviera en pruebas, como manifiesta el Ayuntamiento, por lo que, en caso de hallarse en esta fase, ello no fue informado a los trabajadores. No obstante, como ya hemos indicado, ello es indiferente a efectos de obligaciones en materia de protección de datos, que serían igualmente aplicables a la fase de pruebas que a la definitiva.

- En ninguno de los carteles consta la información exigida por el artículo 13 del RGPD: datos del responsable del tratamiento, del delegado de protección de datos, el dónde obtener información adicional y cómo, plazo conservación datos, dónde ejercer los derechos del artículo 15 a 22 del RGPD…etc). Tampoco se ha aportado documento alguno que acredite que dicha información se entregó individualmente a cada empleado antes de registrar su huella dactilar.

En definitiva, de los documentos obrantes en el expediente, se desprenden evidencias suficientes de que la dirección de la residencia estuvo recogiendo las huellas dactilares de sus empleados laborales y las utilizó para que estos registrasen la entrada y salida de su jornada durante casi un año y medio sin haberles informado previa ni posteriormente a la recogida de las huellas de todos los aspectos exigidos a efectos de protección de datos, por lo que se confirma que el Ayuntamiento cometió también una infracción del artículo 13 del RGPD.

VI

Tipificación de las infracciones y calificación a los efectos de la prescripción.

Tal y como ha sido expuesto en los Fundamentos de derecho III a VI de esta resolución, se considera que el Ayuntamiento de Fuentepelayo ha cometido las siguientes infracciones de la normativa vigente en materia de protección de datos:

6. 1. Infracción del artículo 35 del RGPD

Tal y como se ha expuesto en el Fundamento de Derecho III, de conformidad con los hechos probados en el presente procedimiento, se considera que los hechos expuestos vulneran lo establecido en el artículo 35 del RGPD, lo que supone 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."*

6. 2. Infracción del artículo 9 del RGPD.

Tal y como se ha expuesto en el Fundamento de Derecho IV, de conformidad con los hechos probados en el presente procedimiento, se considera que los hechos expuestos vulneran lo establecido en el artículo 9 del RGPD, lo que supone 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*."

6. 3. Infracción del artículo 13 del RGPD.

Tal y como se ha expuesto en el Fundamento de Derecho V, de conformidad con los hechos probados en el presente procedimiento, se considera que los hechos expuestos vulneran lo establecido en el artículo 13 del RGPD, lo que supone 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.h), que:

> *"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:*
> *h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica"*

VII
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, y habiéndose confirmado la comisión de las citadas infracciones, procede dictar resolución declarando la comisión por el Ayuntamiento de Fuentepelayo de 3 infracciones administrativas por la vulneración del Artículo 9 del RGPD, Artículo 35 del RGPD y Artículo 13 del RGPD, tipificadas en el Artículo 83.4.a) del RGPD, Artículo 83.5.a) del RGPD y Artículo 83.5.b) del RGPD. La sanción que corresponde imponer es la declaración de infracción.

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 FUENTEPELAYO, con NIF P4010000J, ha infringido lo dispuesto en el Artículo 9 del RGPD, Artículo 35 del RGPD y Artículo 13 del RGPD, lo que supone la comisión de 3 infracciones administrativas tipificadas en el Artículo 83.4.a) del RGPD, Artículo 83.5.a) del RGPD y Artículo 83.5.b) del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a ***AYUNTAMIENTO DE FUENTEPELAYO***.

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

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

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