- **Expediente N.º: EXP202208695**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Con fecha 11 de julio de 2022 ***A.A.A.*** (en adelante, la parte reclamante) interpuso reclamación ante la Agencia Española de Protección de Datos.

La reclamación se dirige contra DIPUTACIÓN PROVINCIAL DE CUENCA con NIF P1600000B (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

El sistema de control de presencia en la Administración reclamada se ha realizado en los últimos años mediante un procedimiento de autenticación con usuario/contraseña en la Intranet.

A partir del mes de junio, la parte reclamada instaló diversos dispositivos y marcas con el propósito de establecer un nuevo sistema de control de los fichajes basado en la huella dactilar.

Afirma que no recibió ninguna información relativa a los procedimientos de seguridad vinculados al tratamiento de sus datos biométricos.

Acompaña a la reclamación un escrito presentado electrónicamente el día 08/06/2022, con número de entrada 10475/2022, modelo "Solicitud Genérica de Empleados de Diputación de Cuenca", solicitando información al respecto.

Manifiesta que el tratamiento de los datos biométricos atenta contra los derechos y libertades de los trabajadores y que en caso de que se produzca un incidente de seguridad el daño es irreversible, puesto que se utiliza un sistema operativo obsoleto.

Pregunta por qué se vuelve a implantar un sistema basado en la huella dactilar si existen otras alternativas menos intrusivas y proporcionales.

En particular, solicita:

1.- Información sobre el cumplimiento del RGPD.
2.- Información y/o copia del análisis de riesgos realizado.
3.- Información y/o copia del EIPD, en caso de haberse realizado.
4.- Información sobre las medidas de seguridad implantadas en base al análisis de riesgos.
5.- En el caso de que el EIPD y/o el análisis de riesgos realizado haya determinado un riesgo alto, solicita la supresión de los datos biométricos del sistema.

Manifiesta que ha transcurrido un mes sin recibir contestación.

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 16 de agosto de 2022, se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

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 16 de agosto de 2022, como consta en el acuse de recibo que obra en el expediente.

Con fecha 16 de septiembre de 2022 se recibe en esta Agencia escrito de respuesta de la DIPUTACIÓN PROVINCIAL DE CUENCA, indicando lo siguiente:

"La Diputación provincial de Cuenca, con fecha 9 de agosto de 2.018, formalizó contrato administrativo de servicios cuyo objeto era el "servicio de soporte y mantenimiento de WCCRONOS (CONTROL DE PRESENCIA)", siendo la adjudicataria, después del correspondiente procedimiento de licitación, la mercantil ABACO C.E. INFORMÁTICOS S.L.

Se acompaña al presente escrito el contrato formalizado entre las partes. En relación con el sistema de control de presencia instalado por dicha empresa en ejecución del contrato, la empresa adjudicataria puso de manifiesto y se ha ratificado en que "NUNCA se guarda la imagen de la huella y NUNCA se puede reproducir dicha imagen".

En concreto, se nos informa que el funcionamiento del sistema es el siguiente:

- Se guarda/almacena un número que genera un algoritmo en función de la fisonomía de la huella (a través de las llamadas minucias, crestas, valles, …) y dicho número se asocia al código del trabajador (en nuestro caso, el empleado público).

- La HUELLA NO SE GUARDA NUNCA. En resumen, se especifica que la huella como tal no se almacena ni se puede reproducir. Se adjunta informe emitido por el Administrador único de ABACO C.E. INFORMÁTICOS S.L.

Asimismo, se ha remitido por esta empresa a la Diputación informe elaborado por la mercantil que ha suministrado los aparatos utilizados para el control de presencia (SPEC S.A.), en el cual se pone de manifiesto, entre otras consideraciones, sobre protección de la identidad lo siguiente:

"Una vez la huella ha sido escaneada y los puntos característicos (las minucias) han sido extraídos, la imagen escaneada se destruye. Por otra parte, a partir de las minucias es totalmente imposible obtener la imagen original de la huella dactilar".

La reclamación no fue trasladada al Delegado de protección de datos hasta el momento en el que se recibió el requerimiento de la Agencia de protección de datos a la que me dirijo, a la cual se adjunta la mencionada reclamación.

Una vez conocida dicha reclamación, por parte de este Delegado de protección de datos se ha procedido a requerir de los distintos servicios implicados (Recursos Humanos e Informática) toda la información existente sobre la implantación del sistema de control horario y las posibles implicaciones respecto del tratamiento de datos personales, tanto para dar respuesta al requerimiento de la Agencia, como para analizar las implicaciones que dicho control horario podría tener como incumplimiento de la normativa de protección de datos.

La información que se nos ha facilitado por los Servicios implicados es la que hemos expuesto en el punto primero de este escrito. Por otra parte, esta Diputación provincial de Cuenca contrató con una empresa externa (Govertis Advisory Services S.L.) la elaboración de un plan de adecuación e implantación del reglamento general de protección de datos de dicha corporación provincial y fruto de dicho contrato se elaboró la documentación oportuna:

Registro de Actividades de Tratamiento, se efectuó un análisis de riesgo y el correspondiente Evaluación de impacto de protección de datos respecto de los tratamientos que se consideraron que estaban sujetos a la elaboración de esta evaluación, etc.

Por parte de la empresa que elaboró dicha documentación se consideró que el control de horarios implantado por la Diputación provincial no estaba dentro de los supuestos en que era necesaria la elaboración de una EIPD.

Teniendo en cuenta lo expuesto y a la vista de la información recibida, por parte de este Delegado de protección de datos se ha informado de la reclamación al responsable del tratamiento y se ha decidido proceder a analizar si el sistema implantado de control horario afecta al derecho a la protección de datos de los empleados de esta Diputación y, en caso afirmativo, proceder bien a sustituir dicho sistema por uno menos intrusivo o en base a un nuevo análisis de riesgo a elaborar la correspondiente EIPD.

Asimismo se procederá a informar a los empleados públicos sobre las características del sistema de control horario existente y se procederá a dar respuesta al Sr. Romero sobre su solicitud de información."

TERCERO: Con fecha 26 de septiembre de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 10 de febrero de 2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del artículo 35 del RGPD y artículo 13 del RGPD, tipificada en el artículo 83.4 del RGPD y artículo 83.5 del RGPD.

QUINTO: 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), la parte reclamada presentó escrito de alegaciones en el que se manifestaba lo siguiente:

"Volvemos a reiterar lo ya informado en previo escrito de alegaciones presentado el día 16 de septiembre de 2.022 ante dicha Agencia.

En dicho escrito que, según se manifiesta por la propia Agencia, consta en este procedimiento se indica:

"la Diputación provincial de Cuenca, con fecha 9 de agosto de 2.018, formalizó contrato administrativo de servicios cuyo objeto era el "servicio de soporte y mantenimiento de WCCRONOS (CONTROL DE PRESENCIA)", siendo la adjudicataria, después del correspondiente procedimiento de licitación, la mercantil ABACO C.E. INFORMÁTICOS S.L.

Se acompaña al presente escrito el contrato formalizado entre las partes.

En relación con el sistema de control de presencia instalado por dicha empresa en ejecución del contrato, la empresa adjudicataria puso de manifiesto y se ha ratificado en que "NUNCA se guarda la imagen de la huella y NUNCA se puede reproducir dicha imagen".

En concreto, se nos informa que el funcionamiento del sistema es el siguiente:

1 - Se guarda/almacena un número que genera un algoritmo en función de la fisonomía de la huella (a través de las llamadas minucias, crestas, valles, …) y dicho número se asocia al código del trabajador (en nuestro caso, el empleado público).

- La HUELLA NO SE GUARDA NUNCA. En resumen, se especifica que la huella como tal no se almacena ni se puede reproducir.

Se adjunta informe emitido por el Administrador único de ABACO C.E. INFORMÁTICOS S.L.

Asimismo, se ha remitido por esta empresa a la Diputación informe elaborado por la mercantil que ha suministrado los aparatos utilizados para el control de presencia (SPEC S.A.), en el cual se pone de manifiesto, entre otras consideraciones, sobre protección de la identidad lo siguiente:

"Una vez la huella ha sido escaneada y los puntos característicos (las minucias) han sido extraídos, la imagen escaneada se destruye. Por otra parte, a partir de las minucias es totalmente imposible obtener la imagen original de la huella dactilar".

Se adjunta, asimismo, informe emitido por el director del departamento de I + D de la empresa SPEC S.A.".

Partiendo de estas consideraciones, y como se indica en los informes acompañados no se utiliza la huella digital en el sistema de control de acceso de los empleados de la

Diputación provincial de Cuenca, sino que se utiliza un algoritmo que, unido a una clave a introducir en los correspondientes aparatos, procede a la identificación de cada uno de los empleados en el momento de la entrada y la salida.

Es cierto que el algoritmo se consigue en un principio de acuerdo a la fisonomía de una de las partes de la huella digital, las minucias, pero partiendo de las mismas es imposible la obtención original de la huella digital, pues técnicamente una huella digital se compone, además de dichas minucias, de cresta o valle, los cuales no han sido tenidos en cuenta a la hora de proceder a extraer el algoritmo identificador y, en consecuencia, reiteramos no se puede extraer la huella digital que es el dato biométrico que haría identificable a una persona con exclusión de cualquier otra, como establece la normativa de protección de datos.

Por otra parte, consideramos trascendente destacar que el empleado público en el momento en el cual se extraen esas minucias de la huella dactilar está presente y la destrucción de las imágenes es inmediata y realizada en su presencia. Por tanto y dadas estas circunstancias no puede calificarse que dicho sistema de identificación suponga el tratamiento de datos de carácter personal, ni mucho menos de tratamiento de datos de categoría especial, pues en el momento que el correspondiente empleado público se identifica a la hora de acceder o abandonar su puesto de trabajo no se utiliza para su identificación, en ningún caso, la huella dactilar.

Los sistemas biométricos utilizados, no guardan la huella dactilar del individuo como se hace en otro tipo de registros (por ejemplo, en los registros policiales).

Mediante complejos algoritmos matemáticos se genera una plantilla numérica utilizando la información de algunos puntos de la huella.

En ningún caso se puede recuperar la huella a partir de la información de estas plantillas almacenadas, además tampoco se puede deducir a partir de la plantilla características físicas de la huella, el algoritmo de extracción sólo es conocido por el fabricante.

Pues bien, como se desprende de los informes técnicos que constan en esta Diputación provincial, no existe en la misma guardada ninguna huella digital de ninguno de sus empleados públicos y, en consecuencia, no existe riesgo alguno (ni significativo, ni no significativo) para los derechos fundamentales y libertades de los mismos (todo ello al margen de la legitimación de las Administraciones Públicas, e incluso la obligación legal del control horario de sus empleados).

Se considera que no se infringe el deber impuesto en el artículo 13 del RGPD, como se recoge en el acuerdo de iniciación de este procedimiento al que se formulan las presentes alegaciones.

En el mismo sentido, y dada dicha circunstancia, tampoco es exigible a esta Diputación la existencia de una EIPD, como se establece en el acuerdo de iniciación del presente procedimiento sancionador, al no concurrir en el presente caso los requisitos establecidos en el RGPD para la elaboración de dicho instrumento, al no existir riesgo alguno en dicho proceso de identificación, así como tampoco es exigible

el establecimiento de mecanismos adicionales para garantizar los derechos y libertades de los afectados.

Por tanto, entendemos que en el presente supuesto no se han cometido ninguna de las dos infracciones imputadas a esta Diputación provincial en cuanto al concreto hecho del control de presencia de sus empleados."

SEXTO: Con fecha 4 de mayo de 2023, el instructor del procedimiento acordó practicar pruebas donde se dan por reproducidos a efectos probatorios la reclamación interpuesta por ***A.A.A.*** y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones previas de investigación que forman parte del procedimiento AT/03590/2022.

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

SEPTIMO: Con fecha 12 de mayo de 2023 se formuló propuesta de resolución, notificándose por vía electrónica previo aviso en el acuerdo de inicio de que los sucesivos trámites se realizarían por esa vía.

En la propuesta de resolución se propone:

Que por la Directora de la Agencia Española de Protección de Datos se imponga a ***DIPUTACIÓN PROVINCIAL DE CUENCA***, con NIF ***P1600000B***, por una infracción del artículo 35 del RGPD y artículo 13 del RGPD, tipificadas en el artículo 83.4 del RGPD y artículo 83.5 del RGPD una sanción de apercibimiento.

Que por la Directora de la Agencia Española de Protección de Datos se ordene a ***DIPUTACIÓN PROVINCIAL DE CUENCA***, con NIF ***P1600000B***, que en virtud del artículo 58.2.d) del RGPD, en el plazo de un mes, se acredite haber procedido al cumplimiento de ofrecer información a los usuarios cuyos datos personales se recaban para cumplir de ese modo con las exigencias contempladas en el artículo 13 del RGPD, así como la aportación de medios de prueba acreditativos del cumplimiento de lo requerido.

No se han recibido alegaciones por la parte reclamada a dicha propuesta de resolución.

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

HECHOS PROBADOS

PRIMERO: La Diputación Provincial de Cuenca instaló un nuevo sistema de control de los fichajes basado en la huella dactilar, sin remitir a los trabajadores, información relativa a los procedimientos de seguridad vinculados al tratamiento de sus datos biométricos.

SEGUNDO: La parte reclamada considera que el control de horarios implantado por la Diputación provincial no estaba dentro de los supuestos en que era necesaria la elaboración de una evaluación de impacto relativa a la protección de datos. Con ello, se constata que dicha evaluación no ha sido elaborada.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 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

El artículo 4 del el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos, en adelante RGPD), bajo la rúbrica “Definiciones”, dispone que:

“A efectos del presente Reglamento se entenderá por:

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;

2) «tratamiento»: 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;”

III

De los hechos objeto de la presente reclamación se desprende una posible falta de información a los trabajadores del organismo público objeto de reclamación pese al requerimiento presentado por estos.

En este sentido ha de indicarse que el artículo 13 del RGPD, dispone que:

"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 hecho de que se hayan prestado.

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 que no facilitar tales datos;

f) la existencia de decisiones automatizas, 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".

Por su parte, el artículo 11 de la LOPDGDD, dispone lo siguiente:

"1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

a) La identidad del responsable del tratamiento y de su representante, en su caso.

b) La finalidad del tratamiento.

c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679."

Por lo tanto, hemos de considerar que se ha incurrido en una vulneración del artículo 13 del RGPD al no darse a los trabajadores información general sobre la puesta en funcionamiento del nuevo sistema de control de fichajes basado en la huella dactilar, pese a su solicitud el día 08/06/2022, lo cual implicaría una vulneración del derecho a la información reconocido en el artículo 13 del RGPD, e indicado en este fundamento de derecho.

IV

En virtud de lo establecido en el artículo 58.2 del RGPD, la Agencia Española de Protección de Datos, en cuanto autoridad de control, dispone de un conjunto de poderes correctivos en el caso de que concurra una infracción a los preceptos del RGPD.

El artículo 58.2 del RGPD dispone lo siguiente:

"2 Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

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

(...)

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

El artículo 83.5.b) del RGPD establece que:

"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 derechos de los interesados a tenor de los artículos 12 a 22;"

A su vez, el artículo 72. 1 h) de la LOPDGDD, bajo la rúbrica "Infracciones consideradas muy graves dispone:

"1 En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

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."

V

En cuanto al uso de la huella dactilar, objeto también de la presente reclamación, hemos de indicar que los datos biométricos son definidos en el artículo 4.14 del RGPD de la siguiente manera:

"datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;"

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

Cada individuo tiene impresiones dactilares únicas que muestran características específicas que pueden medirse para decidir si una impresión dactilar corresponde con una muestra registrada. Los datos biométricos presentan la particularidad de ser producidos por el propio cuerpo y lo caracterizan definitivamente.

Por lo tanto, son únicos, permanentes en el tiempo y la persona no puede liberarse de ellos, no se pueden cambiar nunca, ni con la edad, creando cuestiones de responsabilidad en caso de compromiso-pérdida o intrusión en el sistema.

Son datos de cuyo uso pueden desprenderse riesgos significativos para los derechos fundamentales y las libertades, y por ello inicialmente está prohibido su uso de conformidad con el artículo 9.1 del RGPD indicándose además en el artículo 9.4 del RGPD que:

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

VI

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

El artículo 28 de la LOPDGDD, señala como obligaciones:

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

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

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

La gestión de riesgos relacionados con las operaciones de tratamiento de datos sujetas al RGPD implica que todas las decisiones relacionadas con dicho tratamiento, y no sólo las vinculadas a la seguridad de estos, se han de sustentar en la gestión de los riesgos. Siempre hay un riesgo inherente al tratamiento, por el hecho mismo de llevarlo a cabo, por ello lo que persigue el proceso de gestión de riesgos es mantenerlo en unos niveles aceptables. Gestionar los riesgos implica evaluarlos y tratarlos.

En el contexto de las AAPP, aparte de las metodologías de análisis de riesgos focalizadas en la seguridad de la información, se han de ampliar para incluir riesgos asociados al incumplimiento de las disposiciones del RGPD.

Las AAPP, en tanto que son responsables del tratamiento de los datos de los ciudadanos, o de sus empleados, antes de poner en marcha nuevas actividades de tratamiento o modificar servicios ya prestados que hagan uso de nuevas tecnologías, deberán identificar aquellos riesgos a los que pueda estar expuesto el tratamiento.

Por ello, todo tratamiento, tanto los ya existentes como los que se pretenda iniciar, deben ser objeto de un análisis de riesgos.

Riesgos que no son estáticos, evolucionan de forma continua, por lo que una vez identificado, exige un esfuerzo de supervisión continua y permanente. La actitud correcta es conocer el riesgo, evaluar sus consecuencias, tomar medidas para minimizarlo y controlar su efectividad en un contexto cambiante.

Este esquema de supervisión continua es lo que se define como la gestión del riesgo.

La evaluación, gestión y minimización del riesgo para los derechos y libertades es una obligación del responsable del tratamiento (artículos 23.2.g, 24.1, 25, 32, 33, 34, 35 y 36 entre otros) y forma parte de la lista de cumplimiento normativo.

El RGPD, aunque da algunas indicaciones, no es concreto a la hora de identificar y pautar cómo realizar la gestión del riesgo de cada tratamiento de forma específica.

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

-Es una herramienta de ayuda al cumplimiento normativo que pretende dar soporte a la decisión y cuya utilización genera la documentación básica en ningún caso exhaustiva sobre la que hay que realizar un análisis y gestión de riesgo por parte de los responsables de cumplir con lo previsto en el RGPD y LOPDGDD.

Está documentación básica será un punto de partida que debe ser completado siguiendo las indicaciones de la guía de gestión de riesgo y evaluación de impacto en tratamiento de datos personales.

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

La Guía para una Evaluación de Impacto en la Protección Datos Personales» que publicó en junio de 2022 en la AEPD, indicaba que existen múltiples metodologías de análisis de riesgos y pueden resultar adecuadas para el objetivo buscado, sin incluir directrices específicas en ese ámbito. Pero por su relevancia y adaptación al caso espe-

cífico de la privacidad, se hizo mención a la publicación "*Methodology for Privacy Risk Management*" de la Commission Nationale de l'Informatique et des Libertés (CNIL), a *MAGERIT* (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), herramienta creada por el Consejo Superior de Administración Electrónica para asistir a los distintos organismos públicos en este ámbito, a Risk IT (ISACA) o ISO 27005, y destacando también a estos efectos la utilidad de las normas ISO 31000 sobre principios y directrices de gestión del riesgo y la norma ISO 31010 sobre técnicas de gestión de riesgos, en la que se detallan diversos métodos que pueden ayudar a identificar y detectar los riesgos de un nuevo producto o servicio.

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

VII

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

El RGPD impone la obligación de disponer de una Evaluación de Impacto en la Protección de los Datos Personales (en adelante EIPD), determinando su artículo 35 del RGPD:

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

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

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

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

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

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

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

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

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

7. La evaluación deberá incluir como mínimo:

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

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

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

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

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

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

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

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

En desarrollo del párrafo 4, la Directora de la AEPD, como una lista no exhaustiva, publicó una lista orientativa de tipos de tratamiento que requieren una evaluación de impacto relativa a la protección de datos, indicándose: *"En el momento de analizar tratamientos de datos será necesario realizar una EIPD en la mayoría de los casos en los que dicho tratamiento cumpla con dos o más criterios de la lista expuesta a continuación, salvo que el tratamiento se encuentre en la lista de tratamientos que no requieren EIPD a la que se refiere en artículo 35.5 del RGPD*."

La lista se basa en los criterios establecidos por las "*DIRECTRICES SOBRE LA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD) Y PARA DETERMINAR SI EL TRATAMIENTO «ENTRAÑA PROBABLEMENTE UN ALTO RIESGO» A EFECTOS DEL RGPD*", adoptadas e 4/04/2017 y revisadas por última vez y adoptadas el 4/10/2017, WP 248 rev.01 del GT 29 que los complementa y debe entenderse como una lista no exhaustiva:

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

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

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

En las mismas Directrices, se señala:

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

"*7. Datos relativos a interesados vulnerables (considerando 75):*

El tratamiento de este tipo de datos representa un criterio debido al aumento del desequilibrio de poder entre los interesados y el responsable del tratamiento, lo cual implica que las personas pueden ser incapaces de autorizar o denegar el tratamiento de sus datos, o de ejercer sus derechos.

Entre los interesados vulnerables puede incluirse a niños (se considera que no son capaces de denegar o autorizar consciente y responsablemente el tratamiento de sus datos), empleados".

Al tratarse el sistema de registro y uso de huellas de sistemas de identificación novedosos y muy intrusivos para los derechos y libertades fundamentales de las personas físicas, el RGPD establece la obligación de gestionar el riesgo que para los derechos y libertades de las personas supone esos tratamientos. Este riesgo surge tanto por la propia existencia del tratamiento, como por las dimensiones técnicas y organizativas del mismo.

El riesgo surge por los fines del tratamiento y su naturaleza, y también por su alcance y el contexto en el que se desenvuelve.

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

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

-La definición del tamaño (cantidad de información) de la plantilla biométrica es una cuestión crucial.

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

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

-No hace falta decir que toda pérdida de las cualidades de integridad, confidencialidad y disponibilidad con respecto a las bases de datos sería claramente perjudicial para cualquier aplicación futura basada en la información contenida en dichas bases de datos, y causaría asimismo un daño irreparable a los interesados.

Por ejemplo, si las huellas digitales de una persona autorizada se asociaran con la identidad de una persona no autorizada, esta última podría acceder a los servicios de que dispone el propietario de las huellas digitales, sin tener derecho a ello.

El resultado sería un robo de identidad, que (independientemente de su detección) quitaría fiabilidad a las huellas digitales de la persona para futuras aplicaciones y, en consecuencia, limitaría su libertad.

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

-Se puede crear la ilusión de que la identificación a través de la huella siempre es correcta, por ello se debe incluir un análisis de los errores que se pueden producir en su uso, medidores de evaluación del rendimiento, tasa de falsa aceptación-probabilidad de que un sistema biométrico identifique incorrectamente a un individuo o

no rechace a un individuo que no pertenece al grupo, y tasa de falso rechazo o falso negativo: no se establece la correspondencia entre una persona y su propia plantilla.

Frente a las decisiones que afecten jurídicamente a una persona, toda decisión que se adopte en base a ello, solo debería efectuarse salvaguardando los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

-Deben adoptarse medidas de seguridad con motivo del tratamiento de datos biométricos (almacenamiento, transmisión, extracción de características y comparación, etc.) y sobre todo si el responsable del tratamiento transmite esos datos a través de Internet.

Las medidas de seguridad podrían incluir, por ejemplo, la codificación de las plantillas y la protección de las claves de codificación aparte del control del acceso y una protección que convierta en virtualmente imposible la reconstrucción de los datos originales a partir de las plantillas.

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

-Se acepta generalmente que el riesgo de reutilización de datos biométricos obtenidos a partir de rastros físicos dejados por personas sin darse cuenta (por ejemplo: huellas digitales) para fines incompatibles es relativamente bajo si los datos no están almacenados en bases de datos centralizadas, sino en poder de la persona y son inaccesibles para terceros.

El almacenamiento centralizado de datos biométricos incrementa asimismo el riesgo del uso de datos biométricos como llave para interconectar distintas bases de datos, lo cual podría permitir obtener perfiles detallados de los hábitos de una persona tanto a nivel público como privado.
Además, la cuestión de la compatibilidad de los fines nos lleva a la interoperabilidad de diferentes sistemas que utilizan la biometría.

La normalización que requiere la interoperabilidad puede dar lugar a una mayor interconexión entre bases de datos.

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

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

La parte reclamada ha manifestado que no se efectuó la EIPD porque una vez la huella ha sido escaneada y los puntos característicos (las minucias) han sido extraídos, la imagen escaneada se destruye.

Asimismo, la Diputación provincial de Cuenca, manifiesta que considera que el control de horarios implantado no está dentro de los supuestos en que sea necesaria la elaboración de una EIPD.

En este sentido se debe indicar que las Directrices del GT 29 sobre la evaluación de impacto relativa a la protección de datos y para determinar si el tratamiento *"entraña probablemente un alto riesgo*" a efectos del Reglamento (UE) 2016/679 adoptadas el 4/04/2017, revisadas por última vez y adoptadas el 4/10/2017, indican sobre las operaciones de tratamiento ya existentes que "*El requisito de realizar una EIPD se aplica a operaciones de tratamiento existentes que probablemente entrañan un alto riesgo para los derechos y libertades de las personas físicas y para las que se ha producido un cambio de los riesgos, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento*".

Además del fundamento de derecho precedente que pone de manifiesto que se ha ejecutado una valoración básica insuficiente y no adecuada de riesgos para los derechos y libertades de los afectados, se debe de añadir que además, una EIPD debe percibirse como un instrumento de ayuda en la toma de decisiones relativas al tratamiento, por lo que es recomendable realizarla en las fases de concepción y diseño del tratamiento.

Con ello se cumpliría con los principios de protección de datos desde el diseño, y ayuda a que las garantías seleccionadas estén guiadas por la gestión del riesgo y se implementen durante la fase de concepción y diseño del tratamiento, estando integradas en el mismo y extendiéndose a todas las etapas de su ciclo de vida.

La protección de datos desde el diseño no es una capa adicional o un elemento que se puede añadir a posteriori.

Por lo tanto, una EIPD, puede implicar que hay que realizar cambios en el tratamiento para introducir modificaciones, garantías o medidas para reducir los riesgos, se ha de realizar antes y durante la fase de diseño, y el enfoque de riesgos que supone la EIPD es un proceso, no un estado.

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

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

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

VIII

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

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

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

La LOPDGDD establece en su artículo 73.t):

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

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

IX

En virtud de lo establecido en el artículo 58.2 del RGPD, la Agencia Española de Protección de Datos, en cuanto autoridad de control, dispone de un conjunto de poderes correctivos en el caso de que concurra una infracción a los preceptos del RGPD.

El artículo 58.2 del RGPD dispone lo siguiente:

"2 Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(…)

b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las

operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;"

(...)

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

(...)

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

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

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

El "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone en su artículo 77 en la redacción vigente en el momento en que se produjeron los hechos:

[…]"

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

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.
(…)
5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo."

En su apartado 1 señala

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

[…]"

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

Por lo tanto, a tenor de lo anteriormente expuesto, esta Agencia considera que nos encontrarnos ante una doble infracción, la primera de conformidad con el artículo 13 del RGPD y la segunda según el artículo 35 del RGPD, indicados en los fundamentos de derecho III y VII respectivamente, como consecuencia de estos dos hechos:

1. La falta de información a los trabajadores relativa al sistema de control de presencia que implica el tratamiento de los datos biométricos de dichos trabajadores de la parte reclamada y

2. La reconocida carencia de Evaluación de Impacto de Protección de Datos por parte de la DIPUTACIÓN PROVINCIAL DE CUENCA.

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 DIPUTACIÓN PROVINCIAL DE CUENCA, con NIF P1600000B, ha infringido lo dispuesto en el artículo 35 del RGPD y artículo 13 del RGPD, infracciones tipificadas en el artículo 83.4 del RGPD y artículo 83.5 del RGPD respectivamente.

SEGUNDO: NOTIFICAR la presente resolución a *DIPUTACIÓN PROVINCIAL DE CUENCA*.

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

CUARTO: Requerir en aplicación de los artículos 90.3 de la LPCAP, y 58. 2.f), del RGPD, a la *DIPUTACIÓN PROVINCIAL DE CUENCA*, con NIF *P1600000B*, para que en el plazo de diez días, "limite *temporal o definitivamente el tratamiento"* del sistema de control horario mediante la huella dactilar, en tanto no disponga de una evaluación de impacto de protección de datos del tratamiento válida, que tenga en cuenta los riesgos para los derechos y libertades de los empleados y las medidas y garantías adecuadas para su tratamiento, o incluso si se realizara, precisara efectuar la previsión de consulta que se establece en el artículo 36 del RGPD e informe a los trabajadores, de la puesta en funcionamiento del nuevo sistema de control de fichajes, basado en la huella dactilar, facilitando la información exigida según el artículo 13 del RGPD.

Transcurrido el tiempo otorgado, deberá informar a esta AEPD.

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

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.

938-010623

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