- **Expediente Nº: PS/00050/2021**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 19 de febrero de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a **SERVICIOS LOGÍSTICOS MARTORELL SIGLO XXI, S.L.** (en adelante la parte reclamada). Notificado el acuerdo de inicio y tras analizar las alegaciones presentadas, con fecha 6 de octubre de 2021 se emitió la propuesta de resolución que a continuación se transcribe:

<<

Expediente nº: PS/00050/2021

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

ANTECEDENTES

PRIMERO: La reclamación interpuesta por **SECCIÓN SINDICAL ****SECCIÓN.1*** (en adelante, el reclamante) tiene entrada con fecha 6/02/2020 en la Agencia Española de Protección de Datos procedente de la Autoridad Catalana de Protección de Datos. La reclamación se dirige contra la empresa, en la que, manifiestan ostentan representación sindical: **SERVICIOS LOGÍSTICOS MARTORELL SIGLO XXI, S.L.,** con CIF B65050247 (en adelante, la reclamada), "*por su oposición a la implementación de un sistema de control presencial de los trabajadores a través de un sistema biométrico de huella digital en las dependencias de la empresa, mediante terminales que incorporan lectores para la captura de la huella dactilar de cada empleado", y "en la actualidad el sistema se conjuga con el lector de tarjeta*".

La reclamada dedica su actividad al "*transporte de ensamblado y montaje de piezas de vehículos automóviles, siendo la empresa SEAT para la que prestan servicios como único cliente*" con unos 520 trabajadores.

Manifiesta el reclamante que, a su juicio, el sistema que se halla en fase de "*pruebas*", no es conforme a la normativa, por:

a) Desproporcionado: "*Las dependencias de la empresa se encuentran ubicadas dentro del recinto de SEAT MARTORELL, que posee su propio sistema de control de ac-*

ceso, visitas y presencia laboral, a los que se deben someter los trabajadores" de la reclamada "*a lo que hay que adicionar el propio sistema de fichaje con tarjeta instaurado en la empresa, por lo que un tercer sistema de control es desproporcionado*."

a) Innecesaria, por la existencia de otros medios menos invasivos para alcanzar el control de presencia.

b) Se pretende igualmente con la implementación del sistema, el control de la producción al haber instalado los lectores en las áreas de trabajo.

c) Ausencia del consentimiento: la empresa obliga a los trabajadores a firmar un documento de consentimiento para el tratamiento de sus datos por lo que no es una manifestación de voluntad libre.

SEGUNDO**:** Con fecha 26/03/2020, se traslada la reclamación a la reclamada, que el 9/07/2020, manifiesta:

1) Al estar ubicada la empresa dentro de las instalaciones del cliente, SEAT, los trabajadores, para acceder, tienen que pasar por el control de acceso a fabrica que su titular tiene implantado. Desde este punto, hasta la ubicación de la empresa reclamada, hay un trayecto andando de unos veinte minutos. Indica que el centro de trabajo tiene una superficie total superior a sesenta mil metros cuadrados, aportando un gráfico con la situación de los puntos de registro horario.

En los espacios donde se implantan los registros de la huella existían históricamente dos terminales de control de presencia mediante tarjeta, que permitían el control de presencia, y el control de la jornada laboral-entradas, salidas y ausencias- y, por otro, la generación de reporte de variables para la elaboración de las nóminas -horas extras, nocturnidades.

Manifiesta que "*durante 2017 con la idea de sustituir estos terminales de tarjeta se instalan cinco terminales de huella en cada una de las áreas de trabajo del centro. Estos nuevos terminales venían a sustituir a los dos de tarjeta con las mismas finalidades y la misma información*". Esta medida se ejecuta con varias premisas:

-para evitar la problemática de que el personal abandone su puesto de trabajo antes de la hora y fiche en la entrada del taller la salida de su turno, y,

- facilitar el proceso de fichaje evitando aglomeraciones en puntos de fichado, pasando de dos a cinco.

Añade que la huella supera a la tarjeta pues evita casos que se han dado de dar la tarjeta entre empleados para fichar por el titular.

Se implantará un solo tipo de registro de presencia de jornada laboral, si bien actualmente coexisten el de tarjeta y el nuevo de huella, están utilizando ambos para comprobar que funciona con corrección antes de implantarlo definitivamente. Indica que van a instaurar un programa para reducir el lapso en que ambos sistemas, tarjeta-huella van a convivir, y van a realizar las nuevas explicaciones del sistema a los trabajadores y a sus representantes.

2) El 13/11/2017, se convocó al Comité de Empresa y se le presentó el proyecto y objetivos

de control de presencia mediante huella, entregándose copia del informe del proveedor de la tecnología, otorgando un plazo para que emitiera su informe. Aporta documentación del acta de la reunión. Indica que el 20/11/2017, efectuaron una segunda reunión en la cual la Sección Sindical de ******SECCIÓN.1***, no así la de ******SECCIÓN.2***, se opuso por considerarla desproporcionada y manifestó que el sistema de tarjeta actual era suficiente y solicitaron un procedimiento de mediación, que no llegó a buen término, y posteriormente, el 15/10/2018, se trasladó por el reclamante la queja a la Inspección de Trabajo. El 14/01/2019, se archivó la queja por no acreditarse infracción. Aporta copia de estos documentos.

3) Manifiesta que de la recogida de las huellas e implantación del sistema se informó a cada trabajador, documentando su entrega con recibí. Aportan copia del del de una empleada, que lleva fecha de 22/01/2018, con el literal "*información por parte de la dirección de la empresa y aceptación por los usuarios del registro de la huella digital*", "*desde la dirección del departamento de recursos humanos se informa a los trabajadores que se ha procedido a la implantación de un sistema de control de accesos visitas y presencia laboral mediante huella dactilar para lo cual se solicitará a los usuarios el registro de la misma y todo ello de conformidad con lo establecido en la ley de Protección de Datos de carácter personal 15/99 de 13/12".*

4) Manifiesta que la publicación del Real Decreto ley 8/2019 de 8/03, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, intensificó las tareas de puesta en marcha del sistema de fichaje, estableciendo un plazo de guardado de datos registrados de cuatro años.

5) Aporta un esquema gráfico del funcionamiento del proceso del tratamiento de la huella dactilar en el que se indica:

a. "*Tras el alta del trabajador y al tiempo que se le informa de la recogida de la huella para control de jornada, un técnico de RRHH toma la huella con el lector denominado* ******LECTOR.1*** *("Sistema basado en minucias: identifica un número limitado de formas de la huella y su posición dentro de la misma. El lector capta la huella y digitaliza unos puntos de referencia y convierte las minucias en una plantilla de huella cifrada (algoritmo)".*

"*Nunca se almacenan imágenes de huella. Esta plantilla de huella no permite la identificación biométrica, solo la verificación biométrica*"

b. Tras la toma de la huella, figura que el "*técnico de recursos humanos asocia en programa* ******PROGRAMA.1*** *la plantilla de huella con ID del empleado*". En el dibujo de ******PROGRAMA.1*** figura que "*almacena datos en el servidor; ID empleado, nombre y apellidos, NIF, plantilla huella cifrada, fecha, hora entrada, hora salida, ausencias*".

c. Desde ******PROGRAMA.1*** hay una doble fecha hacia FICHADORA, y de esta a ******PROGRAMA.1***. *Sobre la FICHADORA, figura: "el trabajador ficha".* Desde ******PROGRAMA.1*** a FICHADORA consta*: "Transferencia automática TCP de trama extra decimal: ID empleado, nombre y apellidos, plantilla huella cifrada*". Desde FICHADORA, en la que figura: "*Almacena datos en el dispositivo: ID empleado, plantilla huella cifrada*", sale la flecha a ******PROGRAMA.1***, figurando: "*Transferencia automática TCP trama extradecimal: ID empleado, fecha, hora entrada, hora salida, au-*

sencias".

Figura un paréntesis explicativo debajo de FICHADORA, que indica:

"La verificación del usuario se realiza en local contra la plantilla cifrada almacenada en la fichadora. Nunca se verifica contra la base de datos central de ******PROGRAMA.1****. Se recogen en automático los datos de fecha y horas. El trabajador registra manualmente con un código las ausencias*".

En el gráfico explicativo, en otra pantalla también figura el flujo cuando se produce la baja del empleado.

6) Manifiesta que analizando los informes del Gabinete Jurídico de la AEPD número 65/2015, 36/2020, de 8/05, y el dictamen 3/2012, del Grupo del artículo 29, sobre "*evolución de las tecnologías biométricas*" se concluye la diferencia de los datos biométricos:

-"*Los de identificación biométrica: La identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir un proceso de búsqueda de correspondencia uno- a- varios*."

-"*Verificación/ autenticación biométrica: la verificación de individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir un proceso de búsqueda de correspondencias uno-a-uno)."*

"*Solamente se tratarían como dato de categoría especial, aquellos en los que se sometan a tratamiento técnico dirigido a la identificación biométrica "uno a varios", y no en el caso de verificación/autentificación biométrica "uno a uno*".

Manifiestan que su sistema es de verificación/autenticación, explicando que sólo se busca la correspondencia de los datos biométricos aportados *en el momento del registro* por el interesado para acreditar que es él*. "Este dato está almacenado en el dispositivo de forma cifrada y es consultado por el sistema de autenticación para verificar que hay una coincidencia".*

"*cuando un empleado pone su dedo en el lector de la fichadora, este dispositivo verifica en local, nunca contra la base de datos central, que se corresponde la plantilla de la huella cifrada que se encuentra almacenada en el dispositivo. En caso de que exista coincidencia, recoge los datos del fichaje- fecha, hora, ID empleado, ausencia, etc.- y los envía al programa de gestión de fichajes* ******PROGRAMA.1****. Se trata de una autenticación, similar a la realizada con una contraseña*".

7) Manifiesta que a la fecha ningún empleado ha ejercido algún tipo de derecho respecto de sus datos.

8) Aporta copia de análisis de riesgos de actividades de tratamiento, (modelo cuestionario y notas al mismo). "*Aplicando como primer paso la adaptación de la herramienta FACILITA RGPD el 8/04/2019 se obtiene el resultado de la actividad de "escaso riesgo*". Indica que evaluaron la necesidad de realizar o no una EIPD. "*El resultado determinó que no se precisaba realizar una evaluación de impacto en protección de datos (EIPD) precisamente por la*

interpretación de que la plantilla de la huella cifrada mediante el algoritmo no debía enmarcarse en los datos especialmente protegidos".

Pero si se realizó un "*análisis de riesgos básicos*" "*para determinar si era preciso implantar procesos y protocolos adicionales a los diseñados*":

-"*16/09/2019, revisión de la probabilidad del riesgo núm5 por oportunidad de mejora en el proceso de borrado detectada a raíz del plan implantación de ISO 27001 pasa valoración*".

-En el apartado de especificar las categorías de datos tratados: "*Se tratan datos de carácter personal de carácter identificativo, plantilla de huella, y de empleado: nombre y apellidos y NIF. Además, se tratan fecha de entrada y salida, y ausencias*".

La conclusión del análisis indica: "*es de riesgo escaso*", "*cuando un empleado pone su dedo en el lector de la fichadora, el propio dispositivo verifica que se corresponde a la plantilla de la huella que se encuentra almacenada en el dispositivo. En el caso de que exista coincidencia, recoge los datos del fichaje: fecha, hora ID del empleado, ausencia, etcétera, y los envía al programa de gestión de fichajes* ******PROGRAMA.1***".

"Se considera que se trata de una autenticación similar a la realizada con una contraseña y no de una identificación biométrica por lo que no se considera un dato especialmente protegido cómo será la imagen completa de una huella que permitirá identificar a un trabajador dentro de una bolsa completa de personas".

TERCERO: La Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante el 7/09/2020.

CUARTO: En el marco de las actuaciones practicadas por la Subdirección General de Inspección de Datos, con objeto de aclarar la respuesta de la reclamada, con fecha 23/11/2020, se le solicitó su colaboración, para que informara sobre el sistema de registro de huella que utilizan.

1) Se les solicita que expliquen brevemente cómo se produce el sistema de registro y guarda-almacenamiento de la plantilla ¿Qué es ******PROGRAMA.1***?, ¿qué es la base central de ******PROGRAMA.1***?, y si ahí se guarda la plantilla convertida en algoritmo de cada empleado, y qué relación tiene con el dispositivo llamado "*fichadora"*

Con fecha 15/12/2020, se recibe su respuesta en la que manifiesta:

******PROGRAMA.1***, "*servidor principal para la gestión del sistema de presencia, pertenece al "Grupo Sesé" , mismo grupo al que pertenece la reclamada y se implementa a través de una aplicación comercial llamada* ******PROGRAMA.1****, de la empresa TECISA*"."*La información para la gestión se almacena en una base de datos incluida con la aplicación, y es en esta base de datos qué tiene la aplicación, dónde se guarda codificada la plantilla recogida de la huella*".

La fichadora, o terminal remoto "*hace de interfaz entre el empleado y el sistema de* ******PROGRAMA.1*** *para la validación y recogida de información*". Mediante este dispositivo, "*nos validamos en el sistema y recoge información como la hora en la que hemos interactuado, por ejemplo*".

2) En el dibujo del gráfico del proceso "*El trabajador ficha*", y "*fichadora*", figura el literal "*almacena datos en el dispositivo: ID empleado-plantilla huella cifrada*", en tal sentido, aclaren ¿a qué dispositivo se refiere? ¿a la fichadora?, describiendo si así fuera como se almacena la plantilla de todos los empleados en toda y cada una de las cinco que disponen.

Distingue dos fases del proceso, la fase de registro de los datos y la fase de operación de registro de la presencia.

Fase 1, Registro de datos:

-Recursos Humanos registra los datos del empleado y recoge su huella con un lector (denominado en este caso ******LECTOR.1***). "*En el momento de la captura, se genera una plantilla con los puntos característicos de esa huella, que se guarda codificada en la base de datos* ******PROGRAMA.1****. No se almacena la imagen de la huella.*

Cuando se graban los datos, el proceso de sincronización envía los datos necesarios desde la aplicación ******PROGRAMA.1*** *a las fichadoras asociadas -cinco- donde quedan almacenados dichos valores. Los datos que se envían son ID del empleado, nombre y apellidos y la plantilla cifrada."*

Fase 2, Operación:

-"*Cuando un empleado quiere registrar su presencia, coloca el dedo en la fichadora que mediante el lector* ******LECTOR.1*** *incorporado, realiza el mismo proceso comentado en la fase 1 cuando se dio de alta al empleado en el sistema. De forma que realiza una captura de los puntos característicos de la huella del empleado, esta captura se codifica y se compara con la plantilla codificada qué está almacenada en la memoria de la fichadora y asociada al ID del empleado. Si es correcta- ambas plantillas coinciden- la fichadora enviara los datos pertinentes del empleado. Nunca se manda la huella codificada ni el nombre, sólo se envía información relevante para el fichaje: fecha, hora, ID del empleado y cualquier código definido de ausencia. Estos datos son los que se transmiten a la aplicación del* ******PROGRAMA.1*** *para su posterior procesamiento.*"

3) Sobre su manifestación de:

"*La verificación de usuario se realiza en local contra la plantilla cifrada almacenada en la fichadora. Nunca se verifica contra la base de datos central de* ******PROGRAMA.1***"

Se solicita que amplíen información sobre:

a) Si su sistema utiliza la misma plantilla para cada empleado, registrando distintos algoritmos, o plantillas distintas para cada empleado.

Manifiesta que al mencionar plantilla "*se trata en realidad de la información codificada que se ha guardado tras leer la huella, esta no se almacena como imagen, sino que se detectan y guardan entre 25 a 80 minucias -son los puntos de la huella donde termina una línea o se bifurca- estos puntos son los que se codifican y se almacenan como plantilla*. *Cada uno de nosotros tenemos unos puntos diferenciados unos de otros, lo que es suficiente para poder identificarnos y lo que se guarda son estos puntos, por lo que no puede haber dos códigos idénticos."*

a) Explique cómo es posible correlacionar a través del sistema uno a uno (autenticación) la introducción de la huella en la fichadora, con la/s plantilla/s, explique si todas las plantilla/s se hallan en la fichadora. (aparentemente se producirá una validación de huella introducida versus todas las plantillas.)

Reitera que *"Cada fichadora almacena las plantillas y el ID de cada empleado, por lo que cuando un empleado pone la huella ésta se codifica en una plantilla y el sistema realiza la búsqueda para ver cuál es igual a la generada. El proceso se realiza de forma local, no se consulta a la aplicación* ******PROGRAMA.1***"

b) Qué diferencia habría entre que el trabajador fiche en la fichadora y la verificación se hace en local contra la plantilla cifrada almacenada en la fichadora, con que lo haga contra la base de datos central de ******PROGRAMA.1***?

"*No habría diferencia técnica o sí de practicidad. El proceso sería el mismo, solo que en ese caso se debería comparar con todas las plantillas almacenadas y se incrementaría notablemente el tiempo que tomaría en la transmisión de la información de ida y vuelta*".

c) La fichadora, ¿tiene en cada momento un solo paquete de datos identificador de la persona que está fichando o todos los paquetes de todos los trabajadores?

Respondió que "*La fichadora guarda la información de todos los trabajadores del centro, ya que se han configurado para facilitar el fichaje en cualquiera de ellas por parte del trabajador*".

4) En el gráfico, desde "*fichadora*" a "******PROGRAMA.1***", existe una doble flecha en la que se contienen literales: "transferencia automática, TCP de trama *extradecimal etc*.", se solicita que expliquen el significado de dichos extremos en ambos sentidos, y que implican las dobles flechas, si se pudiera entender como que hay una transferencia de datos desde el sistema central hasta la fichadora. (id empleado-nombre/apellidos-huella).

Reitera que: "*Cuando se realiza el alta o modificación de un empleado, se hace desde la aplicación* ******PROGRAMA.1****. Una vez se guardan los datos, el sistema lanza una actualización hacia las fichadoras mediante una trama TCP donde se transmite la información (nombre del empleado, ID del empleado, plantilla de la huella) quedándose registrado en las fichadoras*".

Sólo cuando un empleado realiza un fichaje en la fichadora y tras el proceso de validación, la fichadora, envía la información (ID, fecha y hora, ausencias) a la aplicación de ******PROGRAMA.1***".

Indican que su sistema funciona como el de una contraseña. A tal efecto, deben detallar los elementos de dicha idea, usuario, como se verifica y cuál sería el elemento contraseña, como, y donde se almacenan y como y contra que elemento se produce el emparejamiento.

Responde que comparando la forma tradicional de identificarse a través de usuario/ contraseña, indica que el símil con la huella biométrica es que esta permite una autenticación más fuerte que el simple par usuario/contraseña, ya que los datos biométricos son más complejos de reproducir y romper que una contraseña. Por esa razón, indicaban que se trata como si fuera una contraseña, ya que con la huella "*ningún otro empleado puede suplantar la identidad de otros de forma sencilla. En este caso, el usuario es el ID del empleado y la contraseña es la plantilla de su huella*".

5) Otras cuestiones que consideren aclaratorias o convenientes del sistema que según indican busca la correspondencia de los datos biométricos aportados por el empleado cuando procede a la acción de fichar, con el modo en que se produce el registro de los datos, previa confrontación y coincidencia que manifiesta es de tipo "*autenticación"*.

Manifiesta que el sistema de validación biométrico tiene como único objetivo y finalidad la

identificación inequívoca de un empleado dentro del sistema aportándole garantías al mismo ante cualquier intento de suplantación de su identidad, dificultando la reproducción de la huella por parte de un tercero.

QUINTO: Con fecha 19/02/2021 la Directora de la AEPD acordó:

"*INICIAR PROCEDIMIENTO SANCIONADOR a* **SERVICIOS LOGÍSTICOS MARTORELL SIGLO XXI, S.L***., con CIF B65050247, por la presunta infracción del artículo 35 del RGPD de conformidad con el artículo 83.4 a) del RGPD."*

"*a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería de multa administrativa de 20.000 euros, sin perjuicio de lo que resulte de la instrucción*."

SEXTO: La reclamada efectúa las siguientes alegaciones:

1) Utiliza un patrón de la huella dactilar-basado en minucias, se identifica un número limitado de formas de huella y su posición dentro de la misma, asociándose un algoritmo. El patrón se almacena encriptado, conteniendo la posición y tipo de minucias, no siendo posible "*aplicar ingeniería inversa a las plantillas para recuperar imágenes de las huellas*".

2) "S*e emplea un lector de huella que lee la huella del empleado por primera vez y crea el patrón de puntos, pero no guarda la imagen de la huella como tal, sino un algoritmo derivado de los puntos obtenidos en el patrón. Cuando un trabajador pone su dedo para fichar en la fichadora, el lector lee los puntos y los compara con la base de datos en la que se encuentra el algoritmo, que ha sido almacenado, además, de forma cifrada; lo que lo convierte en un código alfanumérico único asociado al patrón de la huella leída por primera vez. Que el dispositivo lea la huella y la compare contra un patrón cifrado es exactamente el mismo proceso de identificación en una contraseña o tarjeta inteligente, por lo que, al no almacenar la imagen de la huella y hacer la identificación mediante un código, entendemos que no estaríamos hablando de un dato biométrico conforme a la definición del artículo 4.14 RGPD*."

3) "*El sistema utilizado no siempre puede identificar a la persona sin ambigüedad, a diferencia de lo que sucedería si se emplease, por ejemplo, un dato genético que es único. Y ello, puesto que la identificación en el grupo de trabajadores se hace con unas coordenadas que no son únicas en el mundo, por tanto, la identificación del empleado se hace sin utilizar el dato biométrico, es decir, la huella. En conclusión, el patrón de la huella no cumple el requisito de unicidad*." "*Por consiguiente, el patrón de huella del empleado no es un dato biométrico conforme al artículo 4.14 del RGPD, por tanto, no corresponde aplicar el artículo 9 del RGPD como categoría especial de datos en cuanto a la finalidad del tratamiento del dato biométrico*"

4) El sistema de control de presencia y jornada laboral, para implementar el sistema mediante su software de gestión de presencia llamado ******PROGRAMA.1*** se contrató con la empresa TECISA 74, S.L. y la instalación de las fichadoras (******FICHADORAS.1***) que contienen los lectores de huella (******LECTOR.1***) en los accesos a las áreas de trabajo. TECISA utiliza la tecnología de ******LECTOR.1***/IDEMIA en relación con el sistema de identificación mediante huella dactilar.

5) Contrató los servicios de TECISA 74, S.L. por ser un proveedor referente para la Administración Pública, tal y como se pone de manifiesto en la propia página web del proveedor ******URL.1***, de la que se desprende que "*el Ministerio de Justicia de España (Audiencia Na-*

cional), la Secretaría General de Instituciones Penitenciarias del Ministerio del Interior de España, el Ministerio de Empleo y Seguridad Social en el Control de acceso de internos en los Centros de Estancia Temporal de Inmigrantes de Ceuta y Melilla, el Ayuntamiento de Getafe y la Comunidad de Madrid en su Campus para la Justicia han confiado en TECISA 74, S.L. como proveedor de servicios de control de accesos y de presencia." Además, en la misma web, en concreto en el apartado https://www.tecisa.com/quienes-somos, se informa que "*TECISA 74, S.L. es considerada por la Administración Pública Española como la empresa fabricante del mejor software y terminales de control de accesos y presencia laboral, según lo indica en la reciente resolución del concurso de Catálogo de Patrimonio del Estado una vez evaluadas, durante meses, todas las propuestas presentadas por más de 100 empresas. De entre los 195 productos presentados por compañías nacionales e internacionales, los terminales de control de accesos y presencia laboral fabricados por Tecisa han sido, de forma contundente, los mejor valorados por un grupo de expertos del Ministerio de Hacienda y Administraciones Públicas en representación del Estado Españo*l."

La reclamada actuó en la creencia de que la información que se le ha ofrecido por TECISA respecto al tratamiento de huellas era valida y conforme al RGPD. Además, está dispone de una certificación ISO 9001/2015 de sistemas de gestión de calidad, norma internacional que acredita la capacidad para proporcionar regularmente productos y servicios que satisfagan los requisitos del cliente y los legales y reglamentarios aplicables.

Por otro lado, la reclamada cuenta con el certificado ISO IEC 27001/2013, documento dos, "*conforme ha implementado y aplica un sistema de gestión de seguridad de la información que permite el aseguramiento, la confidencialidad e integridad de datos y de sus sistemas que los procesan, además de la evaluación de riesgos y aplicación de controles necesarios para mitigarlos o eliminarlos."*

6) Manifiesta que pese a que la base legal del tratamiento podría ser el artículo 6.1 b) o el 6.1 c), ha optado por solicitar el consentimiento de sus empleados conforme señala el artículo 6.1 a) y 9.2 a) del RGPD.

Consideran que no existe presión a la hora de la prestación del consentimiento si no se presta por los empleados, dado que la reclamada informó primeramente a la representación de los trabajadores del nuevo sistema, quienes a su vez informaron a los empleados de la empresa y que la inmensa mayoría de los empleados no se negó a otorgar su consentimiento ni tan siquiera algunos miembros de ******SECCIÓN.1*** que conforman el comité de empresa que han presentado la presente reclamación, ni tampoco ninguno ha revocado el consentimiento ni se ha opuesto al tratamiento en ningún momento ni tan siquiera la sección sindical ******SECCIÓN.1*** informó a los trabajadores de su desacuerdo en la implantación del sistema.

7) Manifiesta que el control de presencia y el registro de jornada laboral con patrón de huella como indicaron antes, coexistieron con el anterior sistema basado en la utilización del lector de tarjetas, hasta el momento en que se suspendió con motivo del COVID-19, el 14/03/2020 La propia reclamante sección sindical de ******SECCIÓN.1***, reconoce la existencia de los dos sistemas figurando así en el acuerdo de inicio.

Durante la fase de pruebas del nuevo sistema de control de presencia y jornada laboral que se ha visto interrumpida, se pone de relevancia que hay empleados que han hecho uso única y exclusivamente de su tarjeta conforme al control presencial anterior, no utilizando los lectores de huella conforme al nuevo sistema debido a que estaban en funcionamiento los dos sistemas.

Por el total de fichajes de cada mes y los días de referencia, el nuevo sistema de fichaje fue

utilizado por el 40 o el 50% de la plantilla y no la totalidad.

Ya se aportó en actuaciones previas la actuación de la Inspección de Trabajo y Seguridad Social que analizando el sistema de control presencial dactilar no encontró ninguna irregularidad, lo contrario de lo que manifiesta la AEPD.

Añade que no existe una instrucción o circular específica sobre el tratamiento de datos a través de dispositivos biométricos para el control de presencia, que han actuado de buena fe en la creencia de que el sistema de control y jornada era conforme al RGPD.

Llevaron a cabo una auditoría para la certificación 27001/2013 de 2019, en la que se hizo una evaluación y correspondiente análisis de la aplicación ******PROGRAMA.1***.

8) No obstante, y lo que ha motivado el acuerdo de inicio, han llevado a cabo una evaluación de impacto aplicando el criterio de la Agencia de que se está llevando a cabo un tratamiento de un dato biométrico con finalidad de identificación, modificando también el registro de actividad del tratamiento, y aportan documento 3 con la evaluación del impacto y documento 4 con el registro de la actividad de tratamiento modificado.

Indican que la evaluación de impacto se ha efectuado, pese a que el sistema de control de presencia y jornada laboral mediante patrón de huella solo estuvo vigente desde el 16/01/2020 hasta el 14/03/2020, es decir está inoperativo desde antes del traslado del inicio del traslado. Considera que ha venido cumpliendo y observando obligaciones exigibles y pide que se aperciba o en su caso se reduzca a una sanción mínima, considerando también que analizaron previamente en el análisis de riesgos la valoración de si procedía o no a realización de la Evaluación de impacto.

9) Alude a otros expedientes de la AEPD sobre registro con datos biométricos en los que no se ha impuesto la obligación de efectuar evaluación de impacto conforme señala el artículo 35 del RGPD como por ejemplo el PS 7044/2019 contra una Comunidad de propietarios (en realidad se trataría del E77044/2019, no se alcanzan o asignan mas de siete mil expedientes sancionadores en un año) en el que se archivaron las actuaciones sin que conste que dispusiera de evaluación de impacto, según acta de la junta de propietarios que aprobó el 26/09/2017 la instalación de "*tornos con reconocimiento de huella para acceso a instalaciones*" de un Club social con piscina, anejo a la vivienda. En la resolución se indica que existía otra alternativa de acceso a través de un carné con fotografía y no se detalla el sistema técnico de recogida, almacenamiento y almacenamiento y si el sistema de emparejamiento de datos al poner el dedo para entrar era identificación uno-uno, o uno varios, y se expresa que "*la legitimación para el tratamiento de la huella dactilar para el acceso a las instalaciones por parte de la reclamada debemos buscarlo en el artículo 9 y 6 del RGPD*." Añadiendo que no se aplicará la prohibición en virtud del consentimiento, articulo 9.2.a), siendo además de lo detallado, un supuesto distinto al que aquí se valora.

Y señala otro caso similar como el PS 145 /2019 a la Consejería de Educación y Deporte de la Junta de Andalucía, en un caso similar se le impuso un apercibimiento por infracción del artículo 13 sin que hubiera sanción alguna por incumplimiento del art 35 del RGPD.

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

HECHOS PROBADOS

1) La reclamada dedica su actividad al transporte de ensamblado y montaje de piezas de automóviles, siendo la empresa SEAT para la que prestan servicios como único cliente con unos 520 trabajadores. Las dependencias de la empresa se encuentran ubicadas dentro del recinto de su cliente, SEAT. El centro de trabajo tiene una superficie total superior a sesenta mil metros cuadrados, aportando un gráfico con la situación de los puntos de registro horario.

1) Históricamente existían dos terminales de control de presencia mediante tarjeta. Durante 2017, para sustituir estos terminales de tarjeta se instalan cinco terminales de huella en cada área de trabajo del centro, con las mismas finalidades. Cuando la reclamada responde al traslado, 9/07/2020, informó que coexistieron los métodos de fichaje de tarjeta y el nuevo de huella, utilizando ambos para comprobar que funciona con corrección antes de implantar definitivamente la huella.

2) La reclamada acredita haber consultado a la representación sindical el 13/11/2017, antes del uso del sistema de huela dactilar e individualmente a los empleados, desde 22/01/2018, de conformidad con lo establecido en la ley de Protección de Datos de carácter personal 15/99 de 13/12. En alegaciones indicó la reclamada que el uso de la huella se suspendió con motivo del COVID 19, el 14/03/2020, y que solo estuvo vigente desde el 16/01/2020 hasta el 14/03/2020.

3) Los motivos por los que la reclamada prefiere el uso de la huella sobre la tarjeta, son que evita casos que se han dado de dar la tarjeta entre empleados para fichar por el titular, y que se produce una identificación inequívoca del empleado, evitando la suplantación al dificultar la reproducción de la huella por un tercero.

4) La finalidad del registro de huella dactilar es el control horario o de jornada, de conformidad con el artículo 34.9 del Estatuto de los Trabajadores.

5) El sistema de recogida y registro de la huella de los empleados y su uso se divide en dos fases: 1 Registro de datos, 2 Operación de registro de presencia.

Fase 1: se realiza por un técnico de RRHH que con el programa de gestión de fichajes de la aplicación ******PROGRAMA.1*** de la empresa TECISA, y a través de un lector denominado ******LECTOR.1***, recoge la huella, la captura de modo que identifica un numero limitado de formas de la huella y su posición dentro de la misma (minucias) convirtiéndolas en una plantilla de huella cifrada (información codificada, se guardan entre 25 a 80 minucias-puntos de bifurcación o donde termina una línea) . No se almacena la imagen completa de la huella. En la base de datos incluida en la aplicación se asocia y almacena la plantilla de huella con el ID del empleado, nombre y apellidos, NIF. Al grabar los datos, las fichadoras o terminales remotos, cinco en este caso, en un proceso de sincronización asociado a la aplicación, almacenen dichos valores: plantilla cifrada, ID del empleado, nombre y apellidos.

Fase 2: Cuando un empleado quiere registrar su presencia, que puede hacerlo en cualquiera de los cinco terminales o fichadoras-lectores de huella ******LECTOR.1***-, coloca el dedo en la fichadora que mediante el lector ******LECTOR.1*** incorporado, realiza el mismo proceso comentado en la fase 1 cuando se dio de alta al empleado en el sistema. De forma que realiza una captura de los puntos característicos de la huella del empleado, esta captura se codifica y se compara con la plantilla codificada que de cada empleado está almacenada en la memoria de cada fichadora y asociada al ID del empleado. Si es correcta- ambas plantillas coinciden- la fichadora enviara los datos pertinentes del empleado. Nunca se manda la huella

codificada ni el nombre, sólo se envía información relevante para el fichaje: fecha, hora, ID del empleado y cualquier código definido de ausencia. Estos datos son los que se transmiten a la aplicación de ******PROGRAMA.1*** para su posterior procesamiento.

6) La reclamada disponía del documento de análisis de riesgos de actividades de tratamiento, realizado el 8/04/2019, figurando el resultado de la actividad de "*escaso riesgo*", con resultado de que no era preciso realizar una evaluación de impacto en protección de datos (EIPD).

La reclamada indica que estando en funcionamiento los dos sistemas de fichaje, hubo empleados que han hecho uso única y exclusivamente de su tarjeta con control presencial, y otros sobre un 40 o 50% utilizaron la huella.

8) Pese a que se dejó de usar el sistema de recogida de huella para fichaje desde 14/03/2020, tras el acuerdo de inicio, la reclamada modificó el análisis de riesgos de las actividades del tratamiento, y el registro de actividad de tratamiento para convenir que se precisa evaluación de impacto que manifiesta ha efectuado si bien no fue aportado.

FUNDAMENTOS DE DERECHO

I

Los datos biométricos los define el artículo 4.14 del RGPD:

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

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

De acuerdo con la información proporcionada por la reclamada, al introducir la huella en la fichadora, considerando que cada fichadora tiene todas las plantillas almacenadas de todos los empleados, para que fichen en la que deseen, se compara la misma en orden a que franquee el acceso registrando el comienzo o el final. Se estima que la comparación no se produce una contra una, la del empleado que accede con la suya, sino con todas las que están almacenadas, realizando una función de comparación uno a varios cada vez que se entra o sale. En este caso, aunque no se guarde enteramente la imagen de la huella, sino unas

coordenadas, cada una de ellas en la forma de plantilla, es capaz de identificar unívocamente a cada empleado al confrontar en el terminal la toma de la huella con el resto de las existentes. Las funciones que contiene el algoritmo permiten extraer los puntos característicos de la huella para su posterior comparación con una base de datos asociada al conjunto de usuarios previamente almacenado, siendo capaz de identificar a su titular de entre todas las plantillas, tratándose datos de carácter personal basados en el procesamiento de la huella, identificando de forma única a dicha persona.

Los datos biométricos presentan la particularidad de ser producidos por el propio cuerpo y lo caracterizan definitivamente. Por lo tanto, son únicos, permanentes en el tiempo y la persona no puede ser liberada de él, no se pueden cambiar en caso de compromiso-pérdida o intrusión en el sistema etc.

El artículo 9.1 del RGPD, indica:

" *Tratamiento de categorías especiales de datos personales*"

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

Ante el interés creciente en utilizar estos sistemas en ámbitos diferentes y, al tratarse de sistemas de identificación novedosos y muy intrusivos para los derechos y libertades fundamentales de las personas físicas, la constante preocupación de esta autoridad de control es compartida por el resto de las autoridades desde hace años, como ponen de manifiesto el Documento de trabajo sobre biometría, adoptado el 1/08/2003 por el Grupo del 29, o el posterior Dictamen 3/2012, sobre la evolución de las tecnologías biométricas, adoptado el 27/04/2012, y que ha llevado a que el propio legislador comunitario incluya estos datos entre las categorías especiales de datos en el RGPD. De este modo, estando prohibido su tratamiento con carácter general, cualquier excepción a dicha prohibición habrá de ser objeto de interpretación restrictiva.

En este sentido, los considerandos 51 y 52 del RGPD lo ponen de manifiesto: "*Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales*. (52) "*Asimismo deben autorizarse excepciones a la prohibición de*

tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. (...)"

II

Frente a la prohibición de partida del tratamiento de los datos biométricos que identifiquen de manera univoca a las personas del artículo 9.1), señala el artículo 9.2 b) y 9.4)

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

"b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;"

(…)

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

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

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

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

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

De acuerdo con lo establecido, el tratamiento ha de ser necesario para el cumplimiento de obligaciones legales, considerando que los mismos efectos de cumplimiento se satisfacían

antes del sistema de la huella con el uso de las tarjetas, siendo la huella preferida por la reclamada por una serie de cuestiones entre las que no se tuvieron en cuenta el tipo de datos intrusivo que se utilizan, los riesgos y garantías establecidos.

En primer termino, como en cualquier tipo de tratamiento que se lleva a cabo, se ha de acreditar la necesidad del tratamiento de datos a través del registro de huellas y proporcionalidad para el cumplimiento de la obligación legal del registro de jornada. Se considera que pueden existir sistemas alternativos al utilizado que cumplen con los principios de proporcionalidad, necesidad y minimización en el tratamiento de datos. No se explica porque es necesario y preferible el sistema de identificación al de verificación. Para poder utilizar este sistema, de acuerdo con los parámetros establecidos en el RGPD, las empresas u organizaciones necesitan demostrar altos niveles de responsabilidad proactiva y diseño por defecto de Protección de Datos desde antes del tratamiento, incluyendo el hecho de ser capaces de justificar que el sistema utilizado es necesario, proporcionado en cada contexto específico en el que se va a implementar y acreditar que medidas técnicas menos intrusivas no existen o no funcionarían.

El Dictamen 3/2012, sobre la evolución de las tecnologías biométricas, adoptado el 27/04/2012, y que ha llevado a que el propio legislador comunitario incluya estos datos entre las categorías especiales de datos en el RGPD señala que : "*Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar. Un tercer aspecto para ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado".*

El Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del GT29 (adoptado el 8/06/2017) establece que "*aunque el uso de estas tecnologías puede ser útil para detectar o prevenir la pérdida de propiedad intelectual y material de la empresa, mejorando la productividad de los trabajadores y protegiendo los datos personales de los que se encarga el responsable del tratamiento, también plantea importantes retos en materia de privacidad y protección de datos. Por consiguiente, se requiere una nueva evaluación del equilibrio entre el interés legítimo del empresario de proteger su empresa y la expectativa razonable de privacidad de los interesados: los trabajadores*".

Por ello, "*Independientemente de la base jurídica de dicho tratamiento, antes de su inicio se debe realizar una prueba de proporcionalidad con el fin de determinar si el tratamiento es necesario para lograr un fin legítimo, así como las medidas que deben adoptarse para garantizar que las violaciones de los derechos a la vida privada y al secreto de las comunicaciones se limiten al mínimo. Esto puede formar parte de una evaluación de impacto relativa a la protección de datos (EIPD)*".

Antes de implantar un sistema de reconocimiento de huella dactilar, el responsable debe de valorar si hay otro sistema menos intrusivo con el que se obtenga idéntica finalidad. El apartado 72 de la Guía 3/2019 del CEPD "*on processing of personal data through video devices*", establece en este sentido que: "*The use of biometric data and in particular facial re cognition entail heightened risks for data subjects' rights. It is crucial that recourse to such technologies takes place with due respect to the principles of lawfulness, necessity, proportionality and data minimisation as set forth in the GDPR. Whereas the use of these technologies can be perceived as particularly effective, controllers should first of all assess the impact on fundamental rights and freedoms and consider less intrusive means to achieve their legitimate purpose of the processing*".

(*"La utilización de datos biométricos y, en particular, el reconocimiento facial conlleva riesgos mayores para los derechos de los interesados. Es fundamental que el recurso a dichas tecnologías tenga lugar respetando los principios de legalidad, necesidad, proporcionalidad y minimización de los datos establecidos en el RGPD. Considerando que el uso de estas tecnologías puede percibirse como especialmente eficaz, los responsables deberían, en primer lugar, evaluar el impacto en los derechos y libertades fundamentales y*

considerar medios menos intrusivos para lograr su objetivo legítimo de la transformación". La traducción es de la AEPD).

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

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

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

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

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

-Los artículos 16 a 20 del RGPD indican que (cuando el tratamiento de datos se basa en el consentimiento) los interesados tienen derecho a la supresión de los datos cuando el consentimiento se ha retirado.

III

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

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

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

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

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

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

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

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

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

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

7. La evaluación deberá incluir como mínimo:

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

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

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que

se refiere el apartado 1, y

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

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

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

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

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

En desarrollo del párrafo 4, la directora de la AEPD como una lista no exhaustiva, la Directora de la AEP 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*."

"*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."

La finalidad de la evaluación de impacto, dentro del proceso del cumplimiento normativo "*accountability",* supone la toma de responsabilidad propia por lo que se hace con los datos personales y cómo se cumple con los principios, incorporando apropiadas medidas y

registros para ser capaces de demostrar el cumplimiento. Las organizaciones deben demostrar que están cumpliendo con la norma, incluyendo medidas de documentación sobre como son tratados los datos, con que finalidad, hasta cuándo, y documentar los tratamientos y los procedimientos para centrar la cuestión desde un momento temprano de la construcción del sistema de tratamiento. Su implantación posibilita la minimización de riesgos en el momento de tratar los datos, teniendo en cuenta la proporcionalidad de los mismos, la cantidad de datos, etc. Dentro de la EIPD, figurarían las garantías de los derechos que se vean afectados, el análisis de como se ve afectado el derecho, para que antes de proceder al tratamiento se disponga de un documento que avale la gestión posterior, ayudando a identificar y minimizar los riesgos de un proyecto de tratamiento de datos que va a resultar o afectar en este caso en una alto grado de riesgo a los individuos, empleados del reclamado, dada la forma específica del tratamiento la naturaleza del contexto y los propósitos.
La EIPD es un paso necesario para el tratamiento de datos, no siendo el único exigible, es un presupuesto al que se debe añadir el resto de los requisitos legales para el tratamiento, base legitimadora y respeto de los principios fundamentales del tratamiento de datos previsto en el artículo 5 del RGPD.

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

IV

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

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

La LOPDGDD establece en su artículo 73.t):

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

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

V

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

d) ordenar al responsable o encargado del tratamiento que las operaciones de tra-

tamiento 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;"

VI

La determinación de la sanción que procede imponer por la infracción del artículo 35 del RGPD en el presente caso exige observar las previsiones de los artículos 83.1 y.2 del RGPD, preceptos que, respectivamente, disponen lo siguiente:

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias."

"2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

a) las categorías de los datos de carácter personal afectados por la infracción;

b) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
c) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
d) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
e) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción."

Dentro de este apartado, la LOPDGDD contempla en su artículo 76, titulado "*Sanciones y*

medidas correctivas":

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679."

Para la valoración de la sanción, se contemplan los siguientes agravantes:

-La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o el propósito de la operación de tratamiento que afecta a toda la plantilla, unos 500 empleados; (83.2.a RGPD), aunque la reclamada indica que no todos hicieron uso de la huella. El uso del sistema no llega a los dos meses (16/01 a 14/03/2020, si bien se desconoce si se sigue utilizando.)

-Se incluye una falta de diligencia, dado que preparó con tiempo la implantación del sistema y no previó el impacto del sistema implantado (83.2.b RGPD, 83.2.d) RGPD). No se ha aportado el documento de evaluación de impacto que declara se realizó.

En contrapartida se observan se observa que concurre como atenuante que la reclamada es una entidad del sector logístico en el que se tratan datos de sus empleados si bien no concurre "*b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.* (76.2.b LOPDGDD).

Como consecuencia se cuantifica la sanción en 20.000 euros.

Sobre las razones alegadas por la reclamada de que contrató con una empresa española reconocida que provee de software y terminales de control de accesos en su actividad de "*desarrollo, instalación y mantenimiento de sistemas de control de accesos, presencia laboral y sistemas de seguridad*" que además cuenta con certificados ISO (ENAC) y ella

misma dispone de otro certificado, es de señalar que no se tuvo en cuenta la prohibición de datos con excepciones y no se efectuó un tratamiento diseñado desde la cautela del tipo de datos que se trataban, ofreciendo garantías, elementos que no guardan relación con la infracción imputada, no siendo posible por esta razón reducir la cuantía propuesta.

A la vista de lo expuesto se procede a emitir la siguiente:

PROPUESTA DE RESOLUCIÓN

Que por la Directora de la Agencia Española de Protección de Datos se sancione a **SERVICIOS LOGÍSTICOS MARTORELL SIGLO XXI, S.L.**, con CIF B65050247, por una infracción del artículo 35 del RGPD, de conformidad con el artículo 83.4 a) del RGPD, con una multa de 20.000 euros.

Asimismo, de conformidad con lo establecido en el artículo 85.2 de la LPACAP, se le informa de que podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá una reducción de un 20% del importe de la misma. Con la aplicación de esta reducción, la sanción quedaría establecida en 16.000 euros, y su pago implicará la terminación del procedimiento. La efectividad de esta reducción estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de la cantidad especificada anteriormente, de acuerdo con lo previsto en el artículo 85.2 citado, deberá hacerla efectiva mediante su ingreso en la cuenta restringida nº ***ES00 0000 0000 0000 0000 0000*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa, por pago voluntario, de reducción del importe de la sanción. Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para proceder a cerrar el expediente.

En su virtud se le notifica cuanto antecede, y se le pone de manifiesto el procedimiento a fin de que en el plazo de DIEZ DÍAS pueda alegar cuanto considere en su defensa y presentar los documentos e informaciones que considere pertinentes, de acuerdo con el artículo 89.2 de la LPACAP).

926-280721

Angel Carralero Fernández
INSPECTOR/INSTRUCTOR

>>

SEGUNDO: En fecha 19 de octubre de 2021, la parte reclamada ha procedido al pago de la sanción en la cuantía de **16000 euros** haciendo uso de la reducción prevista en la propuesta de resolución transcrita anteriormente.

TERCERO: El pago realizado conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción, en relación con los hechos a los que se refiere la propuesta de resolución.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en el art. 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), la Directora de la Agencia Española de Protección de Datos es competente para sancionar las infracciones que se cometan contra dicho Reglamento; las infracciones del artículo 48 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (en lo sucesivo LGT), de conformidad con lo dispuesto en el artículo 84.3 de la LGT, y las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (en lo sucesivo LSSI), según dispone el artículo 43.1 de dicha Ley.

II

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo LPACAP), bajo la rúbrica “Terminación en los procedimientos sancionadores” dispone lo siguiente:

“1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente.”

De acuerdo con lo señalado, la Directora de la Agencia Española de Protección de Datos
RESUELVE:

PRIMERO: DECLARAR la terminación del procedimiento **PS/00050/2021**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a **SERVICIOS LOGÍSTICOS MARTORELL SIGLO XXI, S.L.**.

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer 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.

968-160721

Mar España Martí
Directora de la AEPD, P.O. la Subdirectora General de Inspección de Datos, Olga Pérez Sanjuán, Resolución 4/10/2021