- Procedimiento Nº: PS/00131/2020

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: D. ***A.A.A.,*** en representación de TRABAJADORES DEL CENTRO INTEGRADO DE FORMACIÓN PROFESIONAL SOMESO (en adelante, el reclamante), con fecha 08/11/2019, interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra CONSELLERÍA DE EDUCACIÓN, UNIVERSIDAD Y FORMACIÓN PROFESIONAL DE LA XUNTA DE GALICIA con NIF ***S1511001H*** (en adelante, el reclamado). Los motivos en que basa la reclamación son: la disconformidad con la implantación de un sistema de control de acceso y horario mediante huella dactilar sin que se les haya informado a los trabajadores de conformidad con lo establecido en la normativa sobre protección de datos de carácter personal.

SEGUNDO: Tras la recepción de la reclamación, la Subdirección General de Inspección de Datos procedió a realizar las siguientes actuaciones:

El 04/12//2019 fue trasladada al reclamado la reclamación presentada para su análisis y comunicación al reclamante de la decisión adoptada al respecto. Igualmente, se le requería para que en el plazo de un mes remitiera a la Agencia determinada información:

- Copia de las comunicaciones, de la decisión adoptada que haya remitido al reclamante a propósito del traslado de esta reclamación, y acreditación de que el reclamante ha recibido la comunicación de esa decisión.

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

- Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares.

- Cualquier otra que considere relevante.

El 09/01/2020 la Consejería en respuesta a la reclamación presentada por los trabajadores manifiesta, en síntesis, que no se ha implantado un sistema de control horario mediante huella dactilar como sistema único de gestión, sino que el uso de la huella dactilar corresponde a una modalidad alternativa y voluntaria a la firma biométrica para los trabajadores, establecida de conformidad con la normativa de protección de datos.

Y aporta: Modelo de consentimiento para el tratamiento de datos biométricos e Información sobre el sistema de gestión de asistencia.

TERCERO: El 30/03/2020, de conformidad con el artículo 65 de la LOPDGDD, la Di-

rectora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante contra el reclamado.

CUARTO: Con fecha 30/09/2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción del artículo 13 del RGPD, tipificada en el artículo 83.5.b) del citado Reglamento y sancionada conforme a lo dispuesto en el artículo 77 de la LOPDGDD.

QUINTO: Notificado el acuerdo de inicio, el reclamado, en fecha 15/10/2020, presentó escrito de alegaciones manifestando lo siguiente: que recibido el acuerdo de inicio se llevó a cabo la investigación de los hechos solicitando información detallada al centro educativo; que son los directores/as de centros docentes públicos de Galicia los que adoptan decisiones concretas de organización y gestión que pueden implicar el tratamiento de datos personales; que en el CIFP Someso se ha implantado un sistema electrónico de gestión de asistencias del personal que presta servicios y debido la forma en que se realizaba dicho control no resultaba efectiva para el adecuado cumplimiento de los fines; que actualmente el sistema electrónico de gestión de asistencias del personal que presta servicio en el CIFP Someso se realiza mediante firma en una tableta o computadora portátil y también una modalidad opcional, más ágil y cómoda, que funciona con el registro de la huella dactilar, cuyo uso está suspendido en la actualidad; que en relación con la Evaluación de impacto realizada, la Consellería está abordando actualmente un proyecto global de adecuación a la normativa de protección de datos, con la finalidad de elaborar un registro de actividades de tratamiento mucho más pormenorizado y completo que el actualmente publicado y que culminará con la realización de las evaluaciones de impacto de aquellos tratamientos en los que sea necesario; que el deber de información fue cumplido poniendo a disposición de todo el personal la información relativa al tratamiento efectuado; que se requirió además a la dirección del centro cese inmediato en el uso del sistema de control de acceso y horario mediante huella dactilar, así como el borrado de los datos biométricos que fuesen recabados a tal objeto y de cualquiera traza de los mismos; que para evitar que puedan reiterarse situaciones similares a la que es objeto de este procedimiento, desde la Consellería se está trabajando en la actualización y ampliación del Protocolo de Protección de Datos en el ámbito educativo con el propósito de conseguir homogeneizar, en lo posible, los requisitos y medidas a adoptar en materia de protección de datos, en las contrataciones llevadas a cabo directamente por los centros docentes.

SEXTO: Con fecha 21/10/2020 se inició un período de práctica de pruebas, acordándose las siguientes

- Dar por reproducidos a efectos probatorios la reclamación interpuesta por el reclamante y su documentación, los documentos obtenidos y generados por los Servicios de Inspección que forman parte del expediente E/11349/2019.

- Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio presentadas por el reclamado y la documentación que a ellas acompaña.

SEPTIMO: El 29/03/2021 fue emitida Propuesta de Resolución en el sentido de que se sancionara al reclamado por infracción del artículo 13 del RGPD, tipificada en el artícu-

lo 83.5.b) del RGPD, con apercibimiento de conformidad con el artículo 77 de la LOPDGDD.

Transcurrido el plazo legalmente señalado al tiempo de la presente Resolución el reclamado no había presentado escrito de alegaciones.

OCTAVO: De las actuaciones practicadas en el presente procedimiento, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: El reclamante presento escrito con fecha de entrada 08/11/2019 en la Agencia Española de Protección de Datos, manifestando su disconformidad con la implantación del sistema de control de acceso y horario mediante huella dactilar por el reclamado sin que a los trabajadores se les haya informado adecuadamente de conformidad con lo establecido en la normativa sobre protección de datos de carácter personal.

SEGUNDO: Consta aportada escrito de 06/11/2019 del reclamante manifestando que los trabajadores del centro de formación profesional les presentaron una reclamación motivada por los siguientes hechos: que a principios del mes de octubre le fue comunicada la implantación de un sistema de control horario basado en la utilización de la huella dactilar sin que les fuese comunicada la información relevante que prescribe el RGPD; que solicitaron a la dirección del centro dicha información relevante como la relativa a identificación del responsable y encargado del tratamiento, del DPD, datos personales puestos a disposición en la elaboración del dicho sistema de control, medidas técnicas y organizativas, etc.; que la respuesta dada por el centro en dos puntos fue genérica señalando que los datos de carácter personal se protegen de acuerdo con la legislación existente.

TERCERO: Consta la respuesta dada por el centro educativo, mediante escrito de 18/10/2019, informando que:

"1. Os datos de carácter persoal de tódolos traballadores do CIFP Someso están protexidos conforme ao prescrito na lexislación vixente e son utilizados única e exclusivamente para a xestión das actividades internas do centro.

2. Tódolos contratos que o CIFP Someso ten firmados coas empresas ue teñen acceso aos ficheiros que conteñen datos de carácter persoal dos traballadores do centro foron celebrados consonte aos requisitos especificados ao efecto na lexislacion vixente".

CUARTO: El reclamado, en escrito de 09/01/2020, señalaba que el CIFP Someso no había *"implantado un sistema de control horario mediante huella dactilar" como sistema único de gestión (como parece dar a entender), sino que el uso de la huella dactilar corresponde a una modalidad de registro alternativa y voluntaria para los trabajadores"* y que se habían cumplido las garantías necesarias para la puesta en marcha de dicho sistema de gestión de asistencias y aportaba el modelo de consentimiento ex-

preso para el tratamiento de datos biométricos y el documento de información a los trabajadores.

QUINTO: El reclamado, en escrito de 15/10/2020, señalaba que: *"Como medida inicial, se requirió además a la dirección del CIPF SOMESO el cese inmediato en el uso del sistema de control de acceso y horario mediante huella dactilar, así como el borrado de los datos biométricos que fuesen recabados a tal objeto y de cualquiera traza de los mismos…"* y que *"A fin de evitar que puedan reiterarse en adelante situaciones similares a la que es objeto de este procedimiento, desde la Consellería se está trabajando en la actualización y ampliación del Protocolo de Protección de Datos en el ámbito educativo con el propósito de conseguir homogeneizar, en lo posible, los requisitos y medidas a adoptar en materia de protección de datos, en las contrataciones llevadas a cabo directamente por los centros docentes…"*

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el art. 58.2 del RGPD y en los art. 47 y 48.1 de LOPDGDD.

II

La legitimación para el tratamiento de la huella dactilar para el control de los trabajadores por parte del empleador debemos buscarlo en el artículo 9 y 6 del RGPD.

El artículo 9 del RGPD establece en sus apartados 1 y 2.b) lo siguiente:

"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 las orientaciones sexuales de una persona física.

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 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."

El artículo 6.1.b) del RGPD indica:

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

(…)

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

El reclamado tiene legitimación, fundamentada en la normativa señalada, para efectuar el control laboral de sus trabajadores y siempre que cumpla los requisitos indicados en el Fundamento de Derecho quinto.

III

Los hechos que motivan la reclamación presentada y que son objeto del procedimiento se concretan en la disconformidad con la implantación de un sistema de control de acceso y horario mediante huella dactilar sin que se les haya informado a los trabajadores de conformidad con lo establecido en la normativa sobre protección de datos de carácter personal.

Estos hechos suponen la vulneración de lo señalado en el artículo 13 del RGPD, al no informar debidamente del tratamiento previsto en relación con el control de fichaje por huella dactilar, de conformidad con lo pronunciamientos establecidos en el citado artículo.

Este artículo determina la información que debe facilitarse al interesado en el momento de la recogida de sus datos, estableciendo lo siguiente:

"Artículo 13. Información que deberá facilitarse cuando los datos personales se obtengan del interesado.

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

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una deci-

sión 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".

IV

En el presente caso, el reclamante manifiesta que a principios del mes de octubre les fue comunicado la utilización de un sistema de control de horario mediante huella dactilar sin que se les hubiera informado debidamente de conformidad con la normativa en materia de protección de datos de carácter personal. Aporta igualmente el escrito remitido a la dirección del centro de formación manifestando su disconformidad y solicitando información al respecto.

Asimismo, consta la respuesta formulada al reclamante en la que se indica en dos puntos, tal y como figura en los hechos probados, que los datos de carácter perso-

nal de todos los trabajadores están protegidos conforme a la legislación vigente y que las empresas que tienen acceso a los ficheros donde figuran los citados datos han sido celebrados con todos los requisitos señalados en la legislación vigente, y de la que se desprende que ni la información transmitida ni el cauce utilizado fuera el más adecuado dada la calidad y especialidad de los datos que estaban en cuestión, pudiendo haber llevado a cabo un mayor esfuerzo en la política de información y comunicación sobre el tratamiento previsto.

En primer lugar, habría que señalar que la implantación e integración de un sistema de control horario basado en la huella dactilar por parte del empleador, ha de ser informado a los empleados de manera completa, clara, concisa y, además, la citada información debe ser completada con referencia tanto a las bases legales que den cobertura a dicho tipo de control de acceso, como a la información básica a la que hace referencia en el artículo 13 del RGPD.

En el caso examinado, la respuesta ofrecida por el centro de formación al escrito presentado por el reclamante, relacionada con el referido control mediante fichaje con huella dactilar, no puede considerarse como la más adecuada.

En segundo lugar, la instalación de un sistema de control basado en la recogida y tratamiento de la huella dactilar de los empleados implica el tratamiento de sus datos personales puesto que dato personal es toda aquella información sobre una persona física identificada o identificable de conformidad con el artículo 4.1 del RGPD.

En cuanto a la huella dactilar se trata, además, de datos que deben ser calificados como datos biométricos y de acuerdo con el artículo 4.14 del RGPD tienen esta consideración cuando han sido *"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".*

Esto hace que, de conformidad con el artículo 9.1 del RGPD, en el caso presente, se les aplique el régimen específico previsto para las categorías especiales de datos previsto en el artículo 9 del RGPD.

En este sentido, el considerando 51 del RGPD pone de manifiesto el carácter restrictivo con el que se puede admitir el tratamiento de estos datos:

"(51) ... 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 liberta-des fundamentales.

Y el considerando 52 señala que

"(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 con-trol de enfermedades transmisibles y otras amenazas graves para la salud… "

De acuerdo con estas consideraciones el tratamiento de datos biométricos de categorías especiales requerirá, además de la concurrencia de una de las bases jurídicas establecidas en el artículo 6 del RGPD, alguna de las excepciones previstas en el artículo 9.2 del RGPD.

El análisis de la base legal de legitimación para realizar este tratamiento viene del artículo 6 del RGPD, relativo a la licitud del tratamiento, que en su apartado 1, letra b) señala: *"El tratamiento será lícito si se cumple al menos una de las siguientes condiciones: (…) b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales (…)".*

En virtud de este precepto, el tratamiento sería lícito y no requeriría el consentimiento, cuando el tratamiento de datos se realice para el cumplimiento de relaciones contractuales de carácter laboral.

Este precepto daría cobertura también al tratamiento de datos de los empleados públicos, aunque su relación no sea contractual en sentido estricto. Hay que señalar que, en ocasiones, para el cumplimiento de sus obligaciones en relación con los empleados públicos, la Administración ha de realizar tratamientos de determinados datos a los que se refiere el RGPD, en su artículo 9, como *"categorías especiales de datos".*

Por otra parte, y tal como pone de relieve el considerando 51 del mismo RGPD, en la medida en que los datos biométricos son de categoría especial en los supuestos de identificación biométrica (art. 9.1 RGPD), será necesario que concurra alguna de las excepciones previstas en el artículo 9.2 del RGPD que permitirían levantar la prohibición general del tratamiento de estos tipos de datos establecida en el artículo 9.1.

En este punto hay que hacer especial mención de la letra b) del artículo 9.2 del RGPD, según la cual la prohibición general de tratamiento de datos biométricos no será de aplicación cuando *"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 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".*

En el ordenamiento español, el artículo 20 del Texto refundido del Estatuto de los trabajadores (TE), aprobado por el Real decreto legislativo 2/2015, de 23 de octubre, prevé la posibilidad de que el empresario adopte medidas de vigilancia y control para verificar el cumplimiento de las obligaciones laborales de sus trabajadores:

"3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y

deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad".

Y en el Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, en su artículo 54 en relación con los principios de conducta de los empleados públicos señala: *"El desempleo de las tareas correspondientes a su puesto de trabajo se realzará de forma diligente y cumpliendo la jornada y el horario establecidos"*

Es innegable la posibilidad de utilización de sistemas basados en datos biométricos para llevar a cabo el control de acceso y horario, aunque tampoco parece que sea o deba ser el único sistema que puede ser usado: así el uso de tarjetas personales, la utilización de códigos personales, la visualización directa del punto de marcaje, etc., que pueden constituir, por sí mismos o en combinación con alguno de los otros sistemas disponibles, medidas igualmente eficaces para llevar a cabo el control.

En cualquier caso, con carácter previo a la decisión sobre la puesta en marcha de un sistema de control de este tipo y teniendo en cuenta sus implicaciones, tratamiento de datos biométricos dirigidos a identificar de manera univoca a una persona física, sería preceptivo llevar a cabo una Evaluación de impacto relativa a la protección de datos de carácter personal para evaluar tanto la legitimidad del tratamiento y su proporcionalidad como la determinación de los riesgos existentes y las medidas para mitigarlos de conformidad con lo señalado en el artículo 35 RGPD.

V

Los datos biométricos están estrechamente vinculados a una persona, dado que pueden utilizar una determinada propiedad única de un individuo para su identificación o autenticación.

Según el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, "Los datos biométricos cambian irrevocablemente la relación entre el cuerpo y la identidad, ya que hacen que las características del cuerpo humano sean legibles mediante máquinas y estén sujetas a un uso posterior."

En relación con ellos, el Dictamen precisa que cabe distinguir diversos tipos de tratamientos al señalar que "Los datos biométricos pueden tratarse y almacenarse de diferentes formas. A veces, la información biométrica capturada de una persona se almacena y se trata en bruto, lo que permite reconocer la fuente de la que procede sin conocimientos especiales; por ejemplo, la fotografía de una cara, la fotografía de una huella dactilar o una grabación de voz. Otras veces, la información biométrica bruta capturada es tratada de manera que solo se extraen ciertas características o rasgos y se salvan como una plantilla biométrica."

El tratamiento de estos datos está expresamente permitido por el RGPD cuando el empresario cuenta con una base jurídica, que de ordinario es el propio contrato de trabajo. A este respecto, la STS de 2 de julio de 2007 (Rec. 5017/2003), que ha entendido legitimo el tratamiento de los datos biométricos que realiza la Administración para el control horario de sus empleados públicos, sin que sea preciso el consentimiento previo de los trabajadores.

Sin embargo, debe tenerse en cuenta lo siguiente:

O El trabajador debe ser informado sobre estos tratamientos.

O Deben respetarse los principios de limitación de la finalidad, necesidad, proporcionalidad y minimización de datos.

En todo caso, el tratamiento también deberá ser adecuado, pertinente y no excesivo en relación con dicha finalidad. Por tanto, los datos biométricos que no sean necesarios para esa finalidad deben suprimirse y no siempre se justificará la creación de una base de datos biométricos (Dictamen 3/2012 del Grupo de Trabajo del art. 29).

O Uso de plantillas biométricas: Los datos biométricos deberán almacenarse como plantillas biométricas siempre que sea posible. La plantilla deberá extraerse de una manera que sea específica para el sistema biométrico en cuestión y no utilizada por otros responsables del tratamiento de sistemas similares a fin de garantizar que una persona solo pueda ser identificada en los sistemas biométricos que cuenten con una base jurídica para esta operación.

O El sistema biométrico utilizado y las medidas de seguridad elegidas deberán asegurarse de que no es posible la reutilización de los datos biométricos en cuestión para otra finalidad.

O Deberán utilizarse mecanismos basados en tecnologías de cifrado, a fin de evitar la lectura, copia, modificación o supresión no autorizadas de datos biométricos.

O Los sistemas biométricos deberán diseñarse de modo que se pueda revocar el vínculo de identidad.

O Deberá optarse por utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.

O Los datos biométricos deben ser suprimidos cuando no se vinculen a la finalidad que motivó su tratamiento y, si fuera posible, deben implementarse mecanismos automatizados de supresión de datos.

VI

El artículo 83.5. b) del RGPD, considera que la infracción de *"los derechos de los interesados a tenor de los artículos 12 a 22",* es sancionable, de acuerdo con el apartado 5 del mencionado artículo 83 del citado Reglamento, *"con multas administrativas de 20.000.000€ 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".*

La LOPDGDD en su artículo 71, I*nfracciones*, señala que:

"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

La LOPDGDD en su artículo 72 indica a efectos de prescripción: *"Infracciones consideradas muy graves:*

"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.

(…)"

VII

No obstante, la LOPDGDD en su artículo 77, *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*, establece lo siguiente:

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

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.

b) Los órganos jurisdiccionales.

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

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

e) Las autoridades administrativas independientes.

f) El Banco de España.

g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.

h) Las fundaciones del sector público.

i) Las Universidades Públicas.

j) Los consorcios.

k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución 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.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica".

En el supuesto que nos ocupa y como se señalaba con anterioridad, el presente procedimiento sancionador evidencia que el reclamado no ha informado adecuadamente en relación con el control de acceso a las instalaciones del centro de formación mediante un sistema de huella dactilar, como sistema alternativo y voluntario al de la firma.

De conformidad con las evidencias de las que se dispone dicha conducta constituye infracción a lo dispuesto en el artículo 13 del RGPD.

El RGPD, sin perjuicio de lo establecido en su artículo 83, contempla en su artículo 77 la posibilidad de acudir a la sanción de *apercibimiento* para corregir los tratamientos de datos personales que no se adecúen a sus previsiones, 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.

No obstante, el reclamado ha manifestado que se requirió a la dirección del CIPF SOMESO el cese inmediato en el uso del sistema de control de acceso y horario mediante huella dactilar, así como el borrado de los datos biométricos que fuesen recabados a tal objeto y de cualquiera traza de los mismos y, además, que se informó al centro de la necesidad de comunicar al delegado de protección de datos de la Conselleria la previsión de contratación de cualquier servicio o suministro que pudiera suponer un tratamiento innovador de datos personales de alumnos o alumnas, de sus familias o del personal del propio centro, a fin de que el delegado de protección de datos pudiera asesorar en tiempo y forma sobre la licitud de dicho tratamiento y supervisar el

cumplimiento del RGPD. Asimismo, se ha señalado que para evitar que puedan reiterarse situaciones similares, desde la Consellería se está trabajando en la actualización y ampliación del Protocolo de protección de Datos en el ámbito educativo para homogeneizar, en lo posible, los requisitos y medidas a adoptar en materia de protección de datos, en las contrataciones llevadas a cabo directamente por los centros docentes.

Por otra parre, también el reclamado ha considerado relevante señalar que:

- Esta plenamente concienciado con la especial sensibilidad de los datos personales tratados por algunos de sus servicios, así como por los centros docentes dependientes de la misma, y en especial, los relacionados con menores.

- Que, entre dichos trabajos de adecuación, se encuentran:

  - La revisión y análisis de cada uno de los tratamientos efectuados, de sus finalidades y bases del tratamiento, que suponen la correspondiente actualización del registro de actividades del tratamiento sobre el ya publicado a la entrada en vigor de la LOPDGDD, y del que se hará difusión a través de la página corporativa de la Xunta de Galicia

  - La revisión y actualización de cláusulas informativas para las personas interesadas (adecuación de las bases legitimadoras del tratamiento especialmente en lo referente a la aplicabilidad del consentimiento) y de las necesarias para regular la relación responsable-encargado del tratamiento o entre corresponsables en su caso.

  - La realización de los correspondientes análisis de riesgos y evaluaciones de impacto sobre la protección de datos.

  - La impartición de sesiones formativas en materia de tratamiento de datos personales dirigidas al personal de la Consellería.

  - Una vez finalizados los trabajos de adecuación, el Delegado de protección de datos de esta Consellería remitirá una circular informativa al respecto dirigida a los usuarios del sistema de información en la que se explicará el estado de dichos trabajos, la principal documentación y normativa en la materia.

Por tanto, a la luz de lo que antecede, se considera que la respuesta del reclamado ha sido razonable y su actuación diligente, subsanando la incidencia no procediendo instar la adopción de medidas adicionales, al haber quedado acreditado la suspensión del sistema de control de acceso mediante huella dactilar, así como el borrado de los datos biométricos que fueron recabados, adoptando otro tipo de medidas de carácter técnico y organizativas de conformidad con la normativa en materia de protección de datos señaladas con anterioridad y evitar que se vuelvan a producir situaciones como la que dio lugar a la presente reclamación, que es la finalidad principal de los procedimientos respecto de aquellas entidades relacionadas en el artículo 77 de la LOPDGDD.

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: IMPONER a CONSELLERÍA DE EDUCACIÓN, UNIVERSIDAD Y FORMACIÓN PROFESIONAL DE LA XUNTA DE GALICIA, con NIF ***S1511001H***, por una infracción del aartículo 13 del RGPD, tipificada en el artículo 83.5.b) del RGPD, una sanción de apercibimiento de conformidad con lo señalado en el artículo 77 de la LOPDGDD.

SEGUNDO: NOTIFICAR la presente resolución a CONSELLERÍA DE EDUCACIÓN, UNIVERSIDAD Y FORMACIÓN PROFESIONAL DE LA XUNTA DE GALICIA, con NIF ***S1511001H***.

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.

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